PERFORMANCE AND SECURITY FOR THE INTERNET OF THINGS

Emerging Wireless Technologies

HAYA SHAJAIAH, AHMED ABDELHADI, AND CHARLES CLANCY

Mc Graw Hill

PERFORMANCE AND SECURITY FOR THE INTERNET OF THINGS

Emerging Wireless Technologies

HAYA SHAJAIAH, AHMED ABDELHADI, AND CHARLES CLANCY

Mc Graw Hill

Performance and Security for the Internet of Things

Emerging Wireless Technologies

Haya Shajaiah, Ph.D.
Ahmed Abdelhadi, Ph.D.
Charles Clancy, Ph.D.

New York Chicago San Francisco Athens
London Madrid Mexico City Milan
New Delhi Singapore Sydney Toronto

Copyright © 2021 by McGraw Hill. All rights reserved. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

ISBN: 978-1-26-046036-0
MHID: 1-26-046036-3

The material in this eBook also appears in the print version of this title: ISBN: 978-1-26-046035-3, MHID: 1-26-046035-5.

eBook conversion by codeMantra
Version 1.0

All trademarks are trademarks of their respective owners. Rather than put a trademark symbol after every occurrence of a trademarked name, we use names in an editorial fashion only, and to the benefit of the trademark owner, with no intention of infringement of the trademark. Where such designations appear in this book, they have been printed with initial caps.

McGraw-Hill Education eBooks are available at special quantity discounts to use as premiums and sales promotions or for use in corporate training programs. To contact a representative, please visit the Contact Us page at www.mhprofessional.com.

Information contained in this work has been obtained by McGraw Hill from sources believed to be reliable. However, neither McGraw Hill nor its authors guarantee the accuracy or completeness of any information published herein, and neither McGraw Hill nor its authors shall be responsible for any errors, omissions, or damages arising out of use of this information. This work is published with the understanding that McGraw Hill and its authors are supplying information but are not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought.

TERMS OF USE

This is a copyrighted work and McGraw-Hill Education and its licensors reserve all rights in and to the work. Use of this work is subject to these terms. Except as permitted under the Copyright Act of 1976 and the right to store and retrieve one copy of the work, you may not decompile, disassemble, reverse engineer, reproduce, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish or sublicense the work or any part of it without McGraw-Hill Education's prior consent. You may use the work for your own noncommercial and personal use; any other use of the work is strictly prohibited. Your right to use the work may be terminated if you fail to comply with these terms.

THE WORK IS PROVIDED "AS IS." McGRAW-HILL EDUCATION AND ITS LICENSORS MAKE NO GUARANTEES OR WARRANTIES AS TO THE ACCURACY, ADEQUACY OR COMPLETENESS OF OR RESULTS TO BE OBTAINED FROM USING THE WORK, INCLUDING ANY INFORMATION THAT CAN BE ACCESSED THROUGH THE WORK VIA HYPERLINK OR OTHERWISE, AND EXPRESSLY DISCLAIM ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. McGraw-Hill Education and its licensors do not warrant or guarantee that the functions contained in the work will meet your requirements or that its operation will be uninterrupted or error free. Neither McGraw-Hill Education nor its licensors shall be liable to you or anyone else for any inaccuracy, error or omission, regardless of cause, in the work or for any damages resulting therefrom. McGraw-Hill Education has no responsibility for the content of any information accessed through the work. Under no circumstances shall McGraw-Hill Education and/or its licensors be liable for any indirect, incidental, special, punitive, consequential or similar damages that result from the use of or inability to use the work, even if any of them has been advised of the possibility of such damages. This limitation of liability shall apply to any claim or cause whatsoever whether such claim or cause arises in contract, tort or otherwise.

To my parents, my beloved husband Islam, and our beloved children Rasem, Tayma, and Yara.

HS

About the Authors

Haya Shajaiah, Ph.D., is currently Adjunct Assistant Professor at George Washington University. She was previously a visiting researcher in the Department of Electrical and Computer Engineering at Virginia Tech. She was awarded an Intelligence Community Postdoctoral Research Fellowship by the Oak Ridge Institute for Science and Education.

Ahmed Abdelhadi, Ph.D., is Assistant Professor at the University of Houston. Before joining UH, he was Research Assistant Professor at Virginia Tech. He was the recipient of the Best Paper Award from the IEEE International Symposium on Systems Engineering (ISSE) in 2019 and the Outstanding Paper Award from the IEEE International Conference on Advanced Communications Technology (ICACT) in 2020.

Charles Clancy, Ph.D., is Senior Vice President for MITRE Labs and Chief Futurist at The MITRE Corporation. He previously served as the Bradley Professor of Electrical and Computer Engineering at Virginia Tech.

Contents

Acknowledgments
Acronyms

1 Introduction
1.1 Motivation and Background
1.2 Security and Performance Challenges in IoT Communications
1.2.1 IoT Spectrum Sharing Systems
1.2.2 Smart Grid Communications
1.2.3 Uplink and Downlink Communications for IoT Applications
1.2.4 M2M Communications
1.3 Previous Studies in Performance and Security of IoT Communications
1.4 Overview
1.5 Book Organization

2 Secure IoT Spectrum Sharing System Leveraging Secure Spectrum Auctions
2.1 Introduction
2.2 System Model
2.2.1 Spectrum Trading Architecture
2.2.2 Spectrum Auction Model
2.3 Design Considerations
2.3.1 The Payment Method
2.3.2 Desired Economic Auction Properties
2.3.3 Design Challenges
2.4 **MTSSA:** Secure Spectrum Auction Design
2.4.1 Paillier Cryptosystem
2.4.2 Frequency Bands Allocation Procedure

2.4.3 Secure Spectrum Auction Using Paillier Cryptosystem
2.5 Numerical Results and Analysis
2.5.1 Performance Analysis
2.5.2 **MTSSA** Security Analysis
2.5.3 **MTSSA** Complexity Analysis
2.6 Conclusion

3 Robust Joint Carrier Aggregation for IoT Spectrum Sharing Systems
3.1 Introduction
3.2 Problem Formulation
3.3 The Global Optimal Solution
3.4 The Dual Problem
3.5 Distributed Optimization Algorithm
3.6 Convergence Analysis
3.6.1 Drawbacks of Algorithms 1 and 2
3.6.2 Solution Using Algorithms 2 and 3
3.7 Numerical Results
3.7.1 First Heterogeneous Network
3.7.2 Second Heterogeneous Network
3.8 Conclusion

4 Optimal Bidding Strategy for Secure Spectrum Auctions
4.1 Introduction
4.2 System Model
4.3 Spectrum Sharing through Secure and Truthful Spectrum Auction
4.3.1 An Optimal Mechanism for Determining True Bidding Values
4.3.2 Spectrum Bands Allocation
4.4 Numerical Results
4.4.1 Bidding Prices and the Final Allocated Rates
4.4.2 Performance Analysis
4.5 Conclusion and Future Work

5 Secure Smart Grids Communications Using Homomorphic Encryption
- 5.1 Introduction
- 5.2 System Model and Design Assumptions
- 5.3 Design Considerations
  - 5.3.1 Payment Rule
  - 5.3.2 Security and Privacy Considerations
  - 5.3.3 Homomorphic Encryption
- 5.4 Secure Power Scheduling Auction Mechanism
- 5.5 Numerical Results
- 5.6 Conclusion

6 Performance Trade-Offs in IoT Uplink Networks under Secrecy Constraints
- 6.1 Introduction
- 6.2 IoT Network Model
  - 6.2.1 Network Connectivity
  - 6.2.2 Uplink Data Transmission Policy
- 6.3 Latency-Centric IoT Uplink Framework
  - 6.3.1 Rate-Limited Backhaul Network
  - 6.3.2 Latency-Limited Backhaul Network
- 6.4 Secrecy in IoT: Attack Models
  - 6.4.1 Passive Eavesdropping on the Backhaul Link
- 6.5 Numerical Results
- 6.6 Conclusion

7 Securing Machine-to-Machine Uplink Communications
- 7.1 Introduction
- 7.2 System Model
- 7.3 Anomaly Detection Metrics
- 7.4 Anomaly Detection and Classification
  - 7.4.1 Distributed Denial-of-Service Attack or Emergency Scenario
  - 7.4.2 Device Failures
- 7.5 Numerical Results

7.5.1 Distributed Denial-of-Service Attack
7.5.2 Emergency Scenario
7.5.3 Device Failures
7.6 Conclusion

8 Conclusion and Future Work

A MATLAB Code for IoT Spectrum Sharing

B MATLAB Code for IoT Smart Grid

References

Index

Acknowledgments

I would like to thank my Ph.D. advisor Prof. T. Charles Clancy and Dr. Ahmed Abdelhadi, my Ph.D. mentor and currently assistant professor at the University of Houston, for co-authoring this book with me and for all their support, advice, help, and guidance. I would not have accomplished this work without their vision and support. I also thank my colleagues Dr. Avik Sengupta and Dr. Akshay Kumar for contributing to some chapters of this book.

I thank all my family members for their support and encouragement. I would like to express my gratitude to my beloved husband, Dr. Islam Younis, for his constant love, support, and encouragement. I have to admit that this work would not have been possible without Islam's support and love. I would also like to express my gratitude to my parents, Dr. Jamal Nouh Shajaiah and Amal Okab, for their encouragement, support, unconditional love, and care. I thank my beloved son Rasem and my beloved daughters Tayma and Yara for the love and happiness they bring to me every day.

Haya Shajaiah, Ph.D.

Acronyms

AS	Application server
BS	Base station
CA	Carrier aggregation
CCs	Component carriers
CSL	Conventional spectrum leasing
DDoS	Distributed denial-of-service
eNodeB	Evolve node B
EPUs	Electric power units
FCC	Federal Communications Commission
4G	Fourth generation
IDS	Intrusion detection scheme
IoT	Internet of Things
LAP	Local access point
LTE	Long-Term Evolution
M2M	Machine-to-machine
MAs	Multiple M2M aggregators
MCD	Modified Canberra distance
MDS	Maximum distance separable
MTSSA-FL	**MTSSA** with fixed limit
NBP	National Broadband Plan
PCAST	President's Council of Advisors on Science and Technology
SAP	Small cell access point
SM	Smart meter
UE	User equipment
VCG	Vickrey-Clarke-Groves
WSPs	Wireless system providers

CHAPTER 1

Introduction

Haya Shajaiah and Ahmed AbdeIhadi

The Internet of Things (IoT) is a network of dedicated physical objects that involves embedded technology used to interact with internal or external environments. IoT is expected to provide connectivity and information exchange anytime and anywhere among a wide variety of physical objects such as sensors, vehicles, and mobile phones [1-4]. IoT is provisioned as a fully connected network paradigm, which is envisioned to create a bridge between machine-type communications (MTCs) and wireless data networks [5]. IoT is a system that includes things, communication, data analysis, and applications. It involves a massive number of objects connected to the Internet [6, 7]. These objects communicate with each other while there are heterogeneous architectures, which challenge the ability to secure IoT communications. Other challenges include reducing the power consumption and minimizing the utilization of resources. IoT applications are found in many fields such as medicine, for example, monitoring patients' pulse rates to keep track of the data and send it to the doctor, industrial plants; for example, quality control, smart cities; for example, bus on the way signals, fitness equipment; for example, keep track of calories to be burnt, and home automation; for example, control of home or room temperature. In IoT, wireless sensor networks are used to sense the objects and send the data through communication channels, which may lead to security issues [8,9]. Security challenges in IoT communications need to be taken into consideration for the design of IoT architectures and protocols [10,11].

1.1 Motivation and Background

We focus on performance and security challenges that affect different types of IoT communications. We propose different mathematical approaches to improve the performance of IoT communications and develop security to counter measurements for different types of IoT security threats. The radio spectrum
allocation plays a very important role in the performance of IoT communications. Due to the recent rapid growth of wireless services, commercial spectrum bands are now overcrowded, while other preassigned-spectrum bands are underutilized. Spectrum sharing enables wireless systems to harvest underutilized swathes of the spectrum, which would vastly increase the efficiency of spectrum usage [12-14]. Making more spectrum available can provide a significant gain in mobile broadband capacity only if those resources can be aggregated efficiently with the existing commercial mobile system resources [15,16]. We introduced a resource allocation based on a carrier aggregation (CA) approach to allocate the network permanent spectrum resources as well as its underutilized spectrum resources based on CA. The proposed approach improved the performance and the quality of the experience for end users.

In addition, to address the limitation in spectrum utilization, spectrum auctions were suggested and proved to be a promising solution to release the underutilized spectrum to potential secondary users. Spectrum auctions are vulnerable to security threats and backroom dealings that result in manipulating the auction. Security issues in spectrum auctions have not been given enough attention in previous research work. In our research project, we designed a secure spectrum auction and developed a spectrum-sharing system that provides an efficient usage of spectrum resources, an essential level of security, privacy, and obfuscation to enable the most efficient and reliable usage of the shared spectrum at a low computational and communication cost. We also studied smart grid security challenges and proposed security and privacy protection methods for smart grid communications. We developed a secure scheduling mechanism for smart grid power resources through an auction process. Communication security for IoT applications is very essential given their wide range of commercial, industrial, and governmental applications. Physical-layer security methods are considered appealing solutions for IoT. However, not all of the existing physical-layer security techniques are suitable for IoT applications. Uplink secrecy in IoT is very essential since the uplink communications contain

data of potentially classified sensor reports. IoT security challenges and their potential solutions have been studied widely in previous research work. However, these studies did not focus on the security of IoT uplink communication. In our research project, we considered the uplink communication of latency-limited industrial IoT networks communicating critical sensor data. We proposed an attack resilient system framework for sensor data reporting on the IoT uplink. Under attacks from an eavesdropper capable of intercepting transmissions on the uplink, we provide countermeasures to such attacks and study the cost of security in terms of latency and backhaul rate. On the other hand, we considered the cyber-vulnerabilities of the IT system for machine-to-machine (M2M) networks being connected to the Internet at large. Since perfect cyber-security and robustness is an idealistic construct, it is worthwhile to design an IDS to quickly detect and mitigate the harmful consequences of cyberattacks. We proposed a novel anomaly detection and classification framework for a general M2M uplink system to detect distributed denial-of-service (DDoS) attacks, emergency scenarios, and terminal device failures.

1.2 Security and Performance Challenges in IoT Communications

1.2.1 IoT Spectrum-Sharing Systems

Traditionally, radio spectrum management is controlled by a central government agency such as the Federal Communications Commission (FCC) in the United States [17]. Such a centralized spectrum assignment mechanism predetermines static bands for specific usage without taking into consideration the service requirements and the dynamic nature of the radio spectrum [18]. This results in an underutilized preassigned-spectrum bands, for example, radar band [19-23]. While many of the commercial bands are overcrowded due to the rapid growth of wireless services. To address this limitation in spectrum utilization, the FCC has legalized secondary markets for the spectrum such that a primary spectrum licensee can lease its underutilized spectrum to secondary incumbents [24-28]. Inspired by microeconomics mechanisms [29-31], the spectrum auction seems to be a promising solution to release the underutilized spectrum to potential secondary users [32, 33]. There has been some previous work to

deal with security issues in auction design. These works have focused on adding some new features to the auction design, such as confidentiality, fairness [34,35], and anonymity.

Because of the reusability feature of the radio spectrum, traditional auctions cannot be directly used in a spectrum auction design [36-38]. Spectrum auctions should allow bidders, that are not within the interference radius of each other, to use the same frequency simultaneously [39-11]. Therefore, the optimal spectrum allocation is considered NP-complete [42-44], whereas conventional auctions are based on optimal allocations [45-47]. In addition, a spectrum auction design is challenged by the effect of the backroom dealing, between insincere bidders and the auctioneer, to the whole network [48-51]. A secure spectrum auction needs to avoid possible frauds of the auctioneer and bid-rigging between the bidders and the auctioneer.

In this work, we present a secure spectrum auction that leverages the Paillier cryptosystem, **MTSSA,** to avoid possible fraud and bid-riggings and provide a framework for a multitier spectrum-sharing system to achieve efficient utilization for the underutilized spectrum. We also present an optimal bidding mechanism for a truthful secure spectrum auction in which bidders are base stations (BSs) that seek to obtain additional temporary resources by participating in the spectrum auction.

In recent years, the number of mobile subscribers and their traffic has increased rapidly [52-57]. Mobile subscribers are currently running multiple applications, simultaneously, on their smart phones that require a higher bandwidth and make users limited to the carrier resources [58-63]. Network providers are now offering multiple services such as multimedia telephony and mobile TV [64-67]. A larger spectrum is required to meet these demands [68,69]. However, it is difficult to provide the required resources with a single-frequency band due to the scarcity of the available radio spectrum [70-72]. Therefore, aggregating different carriers' frequency bands is needed to utilize the radio resources across multiple carriers and allow a scalable expansion of the effective bandwidth delivered to the user terminal, leading to interband noncontiguous CA [73, 74].

CA is one of the most distinct features of the fourth generation (4G) systems including Long-Term Evolution (LTE) Advanced [75, 76]. Given the fact that LTE requires wide carrier bandwidths to utilize such as 10 and 20 MHz, the CA needs to be taken into consideration when designing the

system to overcome the spectrum scarcity challenges [77]. With the CA being defined in [78], two or more component carriers (CCs) of the same or different bandwidths can be aggregated to achieve wider transmission bandwidths between the evolve node B (eNodeB) and the user equipment (UE). An overview of the CA framework and cases is presented in [79]. Many operators are willing to add the CA feature to their plans across a mixture of macro cells and small cells. This will provide capacity and performance benefits in areas where small cell coverage is available while enabling network operators to provide robust mobility management on their macro cell networks.

Increasing the utilization of the existing spectrum can significantly improve network capacity, data rates, and user experience. Some spectrum holders, such as government users, do not use their entire allocated spectrum in every part of their geographic boundaries most of the time. Therefore, the National Broadband Plan (NBP) and the findings of the President's Council of Advisors on Science and Technology (PCAST) spectrum study have recommended making the underutilized federal spectrum available for secondary use [80]. The PCAST Report identifies two technological advances to increase wireless broadband capabilities. First, increasing the deployment of small cell networks, and second using spectrum-sharing technology. Spectrum sharing enables wireless systems to harvest underutilized swathes of the spectrum, which would vastly increase the efficiency of spectrum usage. Making more spectrum available can provide significant gain in mobile broadband capacity only if those resources can be aggregated efficiently with the existing commercial mobile system resources. In this work, we introduce a resource allocation based on a CA approach to allocate the network permanent spectrum resources as well as its underutilized spectrum resources based on CA.

This noncontiguous CA task is challenging. The challenges are both in hardware implementation and joint optimal resource allocation. Hardware implementation challenges are in the need for multiple oscillators, multiple RF chains, more powerful signal processing, and longer battery life [81]. In order to allocate different carriers' resources optimally among mobile users in their coverage areas, a distributed resource allocation algorithm between the UE and the eNodeBs is needed.

A multistage resource allocation with CA algorithms is presented in [82-84]. The algorithm in [82] uses a utility proportional fairness approach to

allocate the primary and the secondary carriers' resources optimally among mobile users in their coverage area. The primary carrier first allocates its resources optimally among users in its coverage area. The secondary carrier then starts allocating optimal rates to users in its coverage area based on the users' applications and the rates allocated to them by the primary carrier. A resource allocation (RA) with a CA optimization problem is presented in [83] to allocate resources from the LTE Advanced carrier and the MIMO radar carrier to each UE, in an LTE Advanced cell based on the application running on the UE for coexistence scenarios [85-90]. A price selective centralized RA with a CA algorithm is presented in [84] to allocate multiple carriers' resources optimally among users while giving users the ability to select one of the carriers to be their primary carrier and the others to be their secondary carriers. The UE's decision is based on the carrier price per unit bandwidth. However, the multistage RA with CA algorithms presented in [82-84] guarantee optimal rate allocation but not optimal pricing.

In this work, we focus on solving the problem of utility proportional fairness optimal RA with joint CA for multicarrier cellular networks. The RA with joint CA algorithm presented in [91] does not converge for high-traffic situations due to the fluctuation in the RA process. In this work, we present a robust algorithm that solves the drawbacks in [91] and allocates multiple carriers' resources optimally among UEs in their coverage area for both high-traffic and low-traffic situations. Additionally, our proposed distributed algorithm outperforms the multistage RA with CA algorithms presented in [82-84], as it guarantees that mobile users are assigned an optimal (minimum) price for resources. We formulate the multicarrier RA with CA optimization problem into a convex optimization framework. We use logarithmic and sigmoidal-like utility functions to represent delay-tolerant and real-time applications, respectively, running on the mobile users' smart phones [92-94]. During the resource allocation process, our distributed algorithm allocates optimal resources from one or more carriers to provide the lowest resource price for the mobile users. In addition, we use a utility proportional fairness approach that ensures nonzero resource allocation for all users and gives real-time applications priority over delay-tolerant applications due to the nature of their applications that require minimum encoding rates. Our model supports both contiguous and noncontiguous CA from one or more network providers and provides an optimal resource allocation solution for spectrum sharing across permanent

licensed and underutilized spectrum resources. The proposed RA method is generic and can be applied to any heterogeneous network. For example, the proposed model can be applied for a cellular system that involves commercial use of the 3.5-GHz spectrum where the system consists of macro cells and small cells. In this case, the proposed resource allocation method can be used to allocate the macro cells' and small cells' resources jointly and optimally among users in their coverage area based on CA.

1.2.2 Smart Grid Communications

The smart grid system has been considered the next generation, promising technology that provides reliable, economic, and environmentally friendly electric services. Many power grids experience a faster growth in the consumption of electric power compared to the expansion rates of generation units. Therefore, maintaining a sufficient reliability of power grids during peak time periods has been given significant attention recently [95]. Demand response in smart grids is one of the promising approaches to improve power grids' reliability. It controls the consumption of electric power by users during peak time periods and usually provides lower overall costs. Price-based demand response is the most commonly used approach that controls and manages users' consumption of electric power by adopting a day ahead [96, 97] or real-time [98, 99] designs for electricity prices. We introduce a new secure electric power management and pricing approach by designing a secure power scheduling auction to schedule the power grid's limited resources for future peak time periods.

We have focused on designing a power auction that has the following auction's favorable economic properties: incentive compatibility, individual rationality, and no positive transfer. An efficient auction design needs to make sure that all bidders submit their true evaluation bidding values in order to ensure truthfulness in the power auction. The proposed power auction uses a payment method that is based on the Vickrey-Clarke-Groves (VCG) auction since VCG is the only auction that has proved to satisfy the above economic properties while maximizing the auctioneer's revenue [100]. Even though the VCG auction has the aforementioned good properties, it is vulnerable to backroom dealing between an insincere auctioneer and greedy bidders who collude with each other to manipulate the auction for their own benefit. For example, the auctioneer may carry out

fraud when he overcharges the winning bidder if that bidder cannot verify the actual submitted bids from other bidders. On the other hand, bid rigging occurs when the auctioneer shares the value of the winning bid with a certain bidder (a greedy bidder) so that the greedy bidder bids more than his true evaluation value to enable the auctioneer to increase his revenue and share the spoils with the greedy bidder. Therefore, the VCG auction cannot be directly used in the power auction, and providing a secure power auction design is becoming necessary. In order to ensure bidders' privacy and avoid possible backroom dealings, a successful secure auction design needs to enable the auctioneer to decide the winners and their charging price without knowing the bidders' actual bids.

1.2.3 Uplink and Downlink Communications for IoT Applications

IoT networks are envisioned to consist of a very large number of low-cost and very low-power devices, for example, sensors installed in an oil pipeline, which mainly communicate by means of small packet payloads in the form of sensor readings over wireless networks to enable monitoring of current conditions like flow rate, pressure, etc. Such widespread industrial applications of IoT often involve communication of small data packets but with very strict latency constraints since stale data (e.g., the instantaneous pressure reading) can have catastrophic consequences. Furthermore, IoT networks will generally have uplink-heavy asymmetric traffic with mostly control signaling in the downlink.

Communication security for IoT applications is very essential given their wide range of commercial, industrial, and governmental applications [101]. It is challenging to implement traditional cryptography methods in IoT systems due to the large number of their MTC devices with heterogeneous access technologies and the subsystems being controlled by different operators. Therefore, physical-layer security methods are considered appealing solutions for IoT [102]. However, due to the nature of MTC devices, not all of the existing physical-layer security techniques are suitable for IoT applications.

1.2.4 M2M Communications

The global M2M market is rapidly expanding with a plethora of booming applications such as smart grids, industrial control systems, and building automation [103-105]. M2M subsystems are increasingly using wireless protocols (such as Zigbee, WirelessHART, GSM, etc.) and thus prone to (passive) eavesdropping attacks and (active) jamming attacks [106]. Also they are vulnerable to cyberat-tacks due to the use of *networked* TCP/IP architecture along with the adoption of IoT technology to reduce its infrastructure and operational costs [107]. Most of the crucial applications operate on commercial off-the-shelf hardware and Windows/Unix operating systems. Thus, M2M systems inherit all the known cyber-threats and vulnerabilities for standard information and communications technology (IT) systems.

Since designing a completely secure and robust M2M system would be expensive and impractical; there exists a nonzero probability of network intrusion by the malicious actors [108]. Therefore, it is important to design intrusion detection schemes (IDS) that can quickly detect a vast array of cyber-threats to mitigate their negative consequences [109].

In this work, we propose a novel anomaly detection and classification framework for a general M2M uplink system. The M2M uplink consists of multiple M2M aggregators (MAs) that aggregate the local sensory traffic, which is eventually processed upstream at an M2M application server (AS). In an M2M uplink, the sensors are usually the most vulnerable to cyberattacks or internal failures, which manifest themselves as anomalies in the local sensor traffic at each MA or in the global traffic at the M2M AS. Therefore, we consider the local (global) anomaly detection engine at MAs (AS), and the detected anomalies are classified using an anomaly classification engine and eventually passed on to a post processing operation that generates an appropriate response to the detected anomalies. The local/global anomaly detection engines employ volumetric and feature-based detection techniques for detecting different anomaly patterns resulting from DDoS attacks, emergency scenarios, and sensor failures.

To overcome the performance limitations of volumetric detection schemes, we propose novel feature-based detection schemes for detecting DDoS attacks, emergency scenarios, and terminal device failures in M2M applications. The detection for DDoS attack and emergency scenarios involves building up a database of legitimate M2M connections during a training phase and then flagging the new M2M connections as anomalies

during the evaluation phase. To distinguish between DDoS attack and emergency scenarios that yield similar signatures for anomaly detection schemes, we propose a modified Canberra distance metric. It basically measures the similarity or differences in the characteristics of inter-arrival time epochs for any two anomalous streams. We detect device failures by inspecting for the decrease in active M2M connections over a reasonably large time interval. Lastly, using Monte Carlo simulations, we show that the proposed anomaly detection schemes have high-detection performance and low-false alarm rate.

1.3 Previous Studies in Performance and Security of IoT Communications

Traditionally, radio spectrum management is controlled by a central government agency such as the FCC in the United States. Such a centralized spectrum assignment mechanism predetermines static bands for specific usage without taking into consideration the service requirements and the dynamic nature of the radio spectrum. This results in underutilized preassigned-spectrum bands, while many of the commercial bands are overcrowded due to the rapid growth of wireless services. To address this limitation in the spectrum utilization, the FCC has legalized secondary markets for the spectrum such that a primary spectrum licensee can lease its underutilized spectrum to secondary incumbents [26]. Inspired by microeconomics mechanisms [29-31], the spectrum auction seems to be a promising solution to release the underutilized spectrum to potential secondary users [32, 33, 45]. There has been some previous work to deal with security issues in auction design. These works have focused on adding some new features to the auction design, such as confidentiality, fairness [34, 35], and anonymity.

Because of the reusability feature of the radio spectrum, traditional auctions cannot be directly used in a spectrum auction design. Spectrum auctions should allow bidders, that are not within the interference radius of each other, to use the same frequency simultaneously. Therefore, the optimal spectrum allocation is considered NP-complete [42, 43], whereas conventional auctions are based on optimal allocations [45].

Most early works in spectrum auctions, such as [33, 45], have focused on single-seller multibuyer auctions that deal with homogeneous channels.

In [45], the authors have proposed **VERITAS,** a truthful mechanism that supports an eBay-like dynamic spectrum market. It is a good fit for short-term and small region-based spectrum auctions which is not the case in FCC-required spectrum auction which is for long-term and large geographical regions. To deal with interference between neighboring bidders, a conflict graph and a wireless spectrum auction framework have been proposed in [45]. Based on these concepts, a conflict graph is used to represent the interference relationship in **VERITAS** [45]. In a sealed secondary price and VCG auctions, the dominant strategy for a certain bidder, when he has no information about other bidders' bids, is to bid with his true evaluation values [100]. The authors in [110] have showed that it is not always right to allocate spectrum bands to the bidder with the highest bid, as proposed in [45], if the sum of the neighbors' bids is much higher than the highest bid. Their proposed solution is based on grouping nodes such that nodes with no interference are grouped together. However, their group partition approach is NP-complete under interference constraints [43].

The authors in [32] have proposed **TRUST,** a spectrum-trading approach that satisfies some good properties. However, it achieves truthfulness while sacrificing one group of bidders, as it takes the group's bid as the clearing price. In [111], the authors have improved the idea of **TRUST** as they succeeded to achieve truthfulness by only sacrificing one buyer in each group. But both works [32,111] have inherited the **McAfee** mechanism [112], which requires homogeneous channels. In [113], the proposed **TASC** mechanism was the first to consider heterogeneous channels. However, it can reduce the system efficiency, as all channels are restricted to a unique clearing price. In [114, 115], **TASC** mechanism has been extended to consider spectrum reusability and diversity of channel characteristics. In [116], the authors have proposed a privacy-preserving auction for spectrum trading. In [117, 118], an auction-based framework is proposed. A third party leases its unused resources to service providers to provide dynamic cellular offloading.

In [45, 115], the authors have exploited the frequency an interference property. They used an interference graph model that makes spectrum allocation, allows spectrum reuse, and avoids interference. In [32, 111], the authors have utilized the reusability property by dividing buyers into groups such that buyers in the same group do not interfere with each other. Each

group of buyers either wins or loses the same channel. In [119], the authors designed a spectrum auction under a physical interference model that allows primary users and secondary users to transmit simultaneously. Both single-minded and multiminded cases are considered. An auction-based spectrum allocation scheme that considers a single primary user and multiple secondary users is proposed in [120]. It uses an exponentially scaled version of the unit price to determine the bidding values. However, none of the aforementioned references considered designing a demand-based optimal bidding mechanism to guarantee a fair and truthful spectrum auction.

Most of existing works have focused on the case of identical spectrum bands. Spectrum reusability in an auction design was first addressed in [32]. In [121], the authors modeled a spectrum auction based on spectrum reusability in a time-frequency division manner. The authors in [122] have also considered spectrum reusability in their auction design by assuming that each spectrum buyer is allowed to have multiple radios. The proposed **MTSSA** scheme also supports the frequency reusability property.

Beside the properties of secondary price auctions that are beneficial to have in a spectrum auction, such as incentive compatibility, individual rationality, and no positive transfers, it is important to secure the spectrum auction to avoid potential backroom dealing. An ideal spectrum auction design would allow the auctioneer to find the best allocation of the frequency bands, determine the winners, and see their payments while the bidders keep their actual bidding values secret and unknown to the auctioneer. This can prevent fraud on the part of insincere auctioneers and bid rigging between the auctioneers and the bidders. There has been some previous work in secure spectrum auctions. The authors in [123-125] have used homomorphic encryption to secure traditional auction designs. In [126], the authors considered frequency reuse in their secure spectrum auction design and propose **THEMIS.** However, **THEMIS** does not support multitier spectrum-sharing systems where spectrum reuse is possible among multiple service providers. In these systems a dynamic spectrum-sharing approach is required to provide efficient sharing of the spectrum among multiple service providers. Furthermore, the computational and communication complexity of **THEMIS** is closely related to the number of available frequency bands. Therefore, **THEMIS** may incur a heavy cost for a large number of frequency bands and bidding values.

There have been several works in the area of resource allocation optimization to utilize the scarce radio spectrum efficiently and improve quality of service (QoS) [127-130]. The authors in [131-134] have used a strictly concave utility function to represent each user's elastic traffic and proposed distributed algorithms at the sources and the links to interpret the congestion control of communication networks. Their work has only focused on elastic traffic and did not consider real-time applications, as it has nonconcave utility functions, as shown in [135]. The authors in [136] and [137] have argued that the utility function, which represents the user application performance, is the one that needs to be shared fairly rather than the bandwidth. In this work, we consider using resource allocation to achieve a utility proportional fairness that maximizes the user satisfaction. If a bandwidth-proportional fairness is applied through a max-min bandwidth allocation, users running delay-tolerant applications receive larger utilities than users running real-time applications, as real-time applications require minimum encoding rates and their utilities are equal to zero if they do not receive their minimum encoding rates. Prior work on QoS for different layers of the Open Systems Interconnection (OSI) model are in [138] for the network layer, in [139,140] for the physical layer, in [141,142] for cross-layer design applied to the LTE third-generation partnership project (3GPP) [143-145], Universal Mobile Terrestrial System (UMTS) [146-148], Mobile Broadband [149,150], and Worldwide Interoperability for Microwave Access (WiMAX) [151-153].

The proportional fairness framework of Kelly introduced in [131] does not guarantee a minimum quality of experience (QoE) [154-157] for each user application. To overcome this issue, a resource allocation algorithm that uses utilityproportional fairness policy is introduced in [158]. We believe that this approach is more appropriate, as it respects the inelastic behavior of real-time applications. The utility-proportional fairness approach in [158] gives real-time applications priority over delay-tolerant applications when allocating resources and guarantees that no user is allocated a zero rate. In [158, 159] and [160], the authors have presented optimal resource allocation algorithms to allocate single-carrier resources optimally among mobile users. However, their algorithms do not support multicarrier resource allocation. To incorporate the CA feature, we have introduced a multistage resource allocation using CA in [82]. In [161] and [162], we present resource allocation with users' discrimination algorithms

to allocate the eNodeB resources optimally among mobile users with elastic and inelastic traffic. In [163], the authors have presented a radio resource block allocation optimization problem using a utility-proportional fairness approach. The authors in [164] have presented an application-aware resource block scheduling approach for elastic and inelastic adaptive real-time traffic where users are assigned to resource blocks.

On the other hand, resource allocation for single-cell multicarrier systems has been given extensive attention in recent years [165-167]. In [168-171], the authors have represented this challenge in optimization problems. Their objective is to maximize the overall cell throughput with some constraints, such as fairness and transmission power. However, transforming the problem into a utility maximization framework can achieve better user satisfaction rather than better system-centric throughput. Also, in practical systems, the challenge is to perform multicarrier radio resource allocation for multiple cells. The authors in [172, 173] suggested using a distributed resource allocation rather than a centralized one to reduce the implementation complexity. In [174], the authors propose a collaborative scheme in a multiple BSs environment, where each user is served by the BS that has the best channel gain with that user. The authors in [175] have addressed the problem of spectrum resource allocation in CA-based LTE Advanced systems, with the consideration of UEs' MIMO capability and the modulation and coding schemes (MCSs) selection. Furthermore, a greedy algorithm has been proposed in [176] for radio resource allocation where the resource assignment is performed jointly for CCs based on proportional fairness. However, their approach is not based on utility proportional fairness, and therefore it does not maximize the system utility. In addition, it does not provide optimal values, as it is based on an approximate algorithm that only achieves part of the proportional fair objective function. In [177], the authors proposed an efficient resource allocation based on a joint CA approach for LTE systems. However, their proposed approach does not consider the different QoS requirements for the users.

Previous research work such as [178-180] proposed pricing algorithms for the operator while assuming that the power grid is operating in normal conditions. In [178], the authors focused on providing a real-time pricing algorithm that maximizes retailer profit when selling electric power to users. They adopted a simulated annealing-based algorithm to compute the

electricity prices. The stochastic approximation approach was used in [179] to design a suboptimal pricing algorithm, whereas in [180] a day-ahead heuristic pricing algorithm is proposed to maximize the operator's profit while considering a noncooperative market.

Security and privacy protection of smart grid communications need to be given more attention. Some efforts have been taken to address smart grid security and privacy issues. Smart grid security challenges were addressed in [181]. A security scheme for a smart grid was proposed in [182] using homomorphic encryption. This approach is based on information aggregation, which makes it limited to that. Homomorphic encryption is adopted in our auction design to provide a sufficient level of privacy to the smart meters and ensures an efficient scheduling mechanism while avoiding possible insincere behaviors of smart meters or the grid operator.

In [183], the authors proposed a sensing security transmission model for IoT systems and presented a feasible framework based on frequency-selective feature of the wireless channel. Securing the data collection process for IoT applications is still a problem for wireless sensor networks, as the traditional cryptography methods are not suitable for IoT distributed data collection process. It is difficult to implement cryptographic methods in IoT due to the wide range of resource-constrained devices and the heterogeneous radio-access technologies [184]. In [185], the security performance of the data collection process were modeled mathematically while the approach characterized the outage probability that the data is successfully intercepted by the malicious eavesdroppers. A securing transmission scheme is designed in [186] for relay communications in IoT networks.

Uplink secrecy in IoT is very essential since the uplink communications contain data of potentially classified sensor reports. IoT security challenges and their potential solutions have been studied widely in previous research work such as in [187, 188]. However, these studies did not focus on the security of IoT uplink communication. In this work, we consider the uplink communication of latency-limited industrial IoT networks communicating critical sensor data. Since the communication of such time-sensitive critical data over IoT networks should ideally be of a confidential nature, the security of such data is an important design paradigm. Recent works in [189,190] have studied secrecy in downlink networks.

A large number of host-based and network-based IDS methods have been developed for IT systems. Host-based systems detect attacks by processing a large amount of internal accounting audit trail data from the users of the system (see [191] and references therein). Network-based systems collect network traffic from a router or switch (see [192] and references therein). These systems can be signature based if they scan network traffic for known attacks with specific bit signatures. Alternatively, they may use machine-learning techniques to mine for anomalous traffic patterns resulting from nonstandard process behavior, which is also the focus of this work but in the context of M2M systems.

The IT systems are confronted with a vast spectrum of traffic anomalies such as DDoS attacks, port scans, equipment failures, flash crowds, etc. This makes automatic anomaly detection and classification particularly challenging. Anomaly detection schemes proposed in the literature are either volumetric schemes built upon measuring the volume of network traffic or feature-based schemes that search for changes in distributional aspects of certain traffic features. Some of the fundamental contributions in this field were made by Lakhina et al. in [193] wherein they presented a general feature-based anomaly detection framework for IP networks using subspace and machine-learning tools. However, these schemes cannot be easily extended to M2M systems due to fundamental differences in their architecture and operational requirements. The field devices, such as sensors, are usually the most vulnerable component of an M2M system due to their limited on-board resources, which preclude the implementation of current cyber-security methods.

Anomaly detection using machine learning tools such as neural networks and k-means has been studied for wireless sensor networks in [194,195]. Kumar in [196] proposed a cluster-analysis-based anomaly detection framework for an M2M network that uses SS7 signaling. Recently, Sedjelmaci et al. [197] studied anomaly detection in an IoT network. They used a game-theoretic approach to intelligently activate the anomaly detection techniques so as to strike a balance between energy consumption and the accuracy of anomaly detection.

1.4 Overview

The contents of this book by topic are as follows.

Security and performance of IoT communications for spectrum sharing systems:

- We develop a secure spectrum auction, **MTSSA,** that considers spectrum reusability and the case of heterogeneous frequency bands, for example, commercial and federal bands. The proposed spectrum auction **MTSSA** has the following properties: it optimizes the usage ofspectrum resources by managing intra-WSP and inter-WSP interference, it provides a truthful auction that is achieved when each bidder submits its true evaluation value, it uses a payment method that satisfies essential economic properties, and it provides a secure spectrum auction that prevents fraud by insincere auctioneers and bid rigging. Simulation results show that **MTSSA** achieves an efficient spectrum utilization, revenue, and bidder satisfaction.
- We present a resource allocation with a joint CA optimization problem that uses a utility-proportional fairness approach and prove that the optimization problem is convex, and therefore the global optimal solution is tractable. We present a robust distributed resource allocation algorithm to solve the optimization problem and provide optimal rates in high-traffic and low-traffic situations.
- We propose an optimal bidding mechanism for determining true bidding values to be used in secure spectrum auctions by BSs that belong to different WSPs participating in a spectrum auction.
- We present a resource allocation based on the CA approach to determine the BS's optimal aggregated rate allocated to each UE, under its coverage area, from both the BS's permanent resources and the BS's winning auctioned spectrum resources. We show through simulation results the performance of the proposed optimal bidding strategy.

Secure smart grids communications using homomorphic encryption:

- We design a secure power-scheduling auction mechanism to schedule the power plant's limited electric power resources during peak hours time slots. The proposed power auction leverages homomorphic encryption through the Paillier cryptosystem to provide a secure and

honest auction mechanism by avoiding possible frauds and bid rigging.
- We show through simulation results the performance of the proposed power scheduling auction and its ability to maximize the performance metrics in order to guarantee a successful power auction.

Performance trade-offs in IoT uplink networks under secrecy constraints:

- We present a latency-centric study of secrecy in latency-limited uplink IoT networks.
- We propose an attack-resilient system framework for sensor data reporting on IoT uplink.
- We provide countermeasures to passive attacks from an eavesdropper capable of intercepting transmissions on the uplink and study the cost of security in terms of latency and backhaul rate.

Securing machine-to-machine uplink communications:

- We present novel feature-based detection schemes for detecting DDoS attacks, emergency scenarios, and terminal device failures in M2M applications.
- We propose a modified Canberra distance metric to distinguish between DDoS attack and emergency scenarios that yield similar signatures for anomaly detection schemes.
- We show that the proposed anomaly detection schemes have a high detection performance and low-false alarm rate.

1.5 Book Organization

The rest of this book is organized as follows. Chapter 2 develops a truthful secure spectrum auction framework by considering the spectrum spatial reuse property and the heterogeneous propagation properties of different frequency bands. The proposed secure spectrum auction leverages Paillier cryptosystem to avoid possible fraud and bid rigging. Chapter 3 presents a robust optimal resource allocation with a joint CA approach to allocate multiple carriers' resources optimally among users with elastic and inelastic

traffic in cellular networks. In Chapter 4, an optimal bidding mechanism is developed for a truthful secure

spectrum auction in which bidders are BSs that seek to obtain additional temporary resources by participating in the spectrum auction. IoT spectrum-sharing MATLAB code is provided in Appendix A. Chapter 5 presents a secure energy trading auction approach to schedule the power plant-limited resources during peak time slots, and the MATLAB code is presented in Appendix B. Chapter 6 provides an attack-resilient system framework for sensor data reporting on IoT uplink, provides countermeasures to passive attacks, and presents the cost of security in terms of latency and backhaul rate. Chapter 7 presents novel feature-based detection schemes for detecting DDoS attacks, emergency scenarios, and terminal device failures in M2M applications to overcome the performance limitations of volumetric detection schemes. Chapter 8 summarizes the contributions presented in this book and points out some future extensions of this work.

CHAPTER 2

Secure IoT Spectrum Sharing System Leveraging Secure Spectrum Auctions[1]

Haya Shajaiah, Ahmed Abdelhadi, and Charles Clancy

The dilemma between the spectrum scarcity and the booming demand for more spectrums has driven the Federal Communications Commission (FCC) to pour out new technologies that allow opportunistic access to the underutilized spectrum bands [199-203]. The FCC has acknowledged the possibility for spectrum licensees to trade their unused spectrum to secondary spectrum markets by leasing it temporarily or on long-term basis [204-207]. An efficient functionality by these secondary spectrum markets can improve spectrum utilization, and therefore increase the spectrum capacity available to wireless service demands. Recently, auction theory has been recognized as a promising tool to solve various spectrum trading problems due to their economically robust allocation efficiency [29-31]. However, traditional auctions cannot be directly applied in a spectrum auction because of the reusability property of the radio spectrum.

Secure spectrum auctions can revolutionize the spectrum utilization of cellular networks and satisfy the ever-increasing demand for resources. In this chapter, we focus on designing a framework for a multitier dynamic spectrum sharing system to provide an efficient sharing of spectrum with commercial wireless system providers (WSPs), with an emphasis on federal spectrum sharing, for example, radar spectrum [208-211]. In this chapter we

present a spectrum sharing system that provides an efficient usage of spectrum resources, manage intra-WSP and inter-WSP interference, and provides essential level of security, privacy, and obfuscation to enable the most efficient and reliable usage of the shared spectrum. The proposed spectrum sharing system features an intermediate spectrum auctioneer responsible for allocating resources to commercial WSPs by running secure spectrum auctions while preventing possible fraud and bid-rigging.

2.1 Introduction

In this chapter, we design a secure spectrum auction framework by considering the spectrum spatial reuse property. We propose **MTSSA,** a secure spectrum auction design that provides framework for a multitier dynamic spectrum sharing system to allocate spectrum resources that are managed by a broker (i.e., the auctioneer). Besides supporting multitier spectrum sharing systems, the computational and communication complexity for the proposed spectrum auction framework is less than other secure spectrum auctions, for example, [126], making it a practical and implementable system. **MTSSA** allows the auctioneer to allocate its underutilized frequency bands that are leased from federal government to commercial WSPs' base stations (BSs) by running secure spectrum auction. By leveraging Paillier cryptosystem, **MTSSA** can prevent possible frauds and bid-rigging.

The major contributions of the proposed spectrum auction are summarized as:

- **MTSSA** considers spectrum reusability and the case of heterogeneous frequency bands, for example, commercial and federal bands.
- **MTSSA** provides a framework for a multitier dynamic spectrum sharing system that allows an efficient spectrum sharing of the underutilized spectrum with commercial WSPs. The auctioneer allocates the underutilized frequency bands to commercial WSPs' BSs by running a secure spectrum auction. **MTSSA** optimizes the usage of spectrum resources by managing intra-WSP and inter-WSP interference. In order to account for frequency reusability, the network is divided into subnets and the auctioneer auctions the

frequency bands in each of the subnets one after another. An intermediate federal gateway maintains a conflict-table for each BS that is updated when changes in frequency bands allocation are made.

- **MTSSA** provides a truthful auction that is achieved when each bidder submits its true evaluation value. Truthfulness is a dominant strategy for **MTSSA** as it prevents manipulating the auction.
- **MTSSA** uses a payment method that satisfies some essential economic properties such as incentive compatibility, individual rationality, and no positive transfers.
- **MTSSA** leverages Paillier cryptosystem [126, 212, 213] to create a ci-phertext for the bidding values. Each BS submits its bidding values through a buffer that creates an encrypted version of the bidding values. While the actual bidding values are kept secret from the auctioneer, the auctioneer is still able to reveal the auction results and charge the bidders securely.
- **MTSSA** provides a secure spectrum auction that prevents frauds of insincere auctioneers and bid-rigging with less computational and communication complexity compared to other secure spectrum auctions, for example, [126]. Simulation results show that **MTSSA** achieves an efficient spectrum utilization, revenue, and bidders' satisfaction.

2.2 System Model

2.2.1 Spectrum Trading Architecture

We consider a spectrum trading scenario where the spectrum owner is a federal regulatory agency that leases its underutilized spectrum, 3.5-GHz ship-borne radar [214-218], on a long-term basis to a broker, which manages spectrum assets and plays the role of a middleman for the spectrum owner of the underutilized spectrum, for example, federal government, and the WSPs. The architecture of these spectrum assignments is represented through a spectrum pyramid, as shown in Figure 2.1. At the top of this pyramid, is the spectrum owner that leases the underutilized frequency bands to a spectrum broker under certain rules [26, 149, 219, 220]. The broker represents a secondary market place that auctions these frequency bands to WSPs. At the bottom of the pyramid are the end users'

devices [i.e., users equipment (UEs)] that are assigned spectrum by the WSPs BSs. In this section we focus on designing a secure spectrum auction between the broker (i.e., the auctioneer) and the WSPs BSs to allocate the underutilized frequency bands.

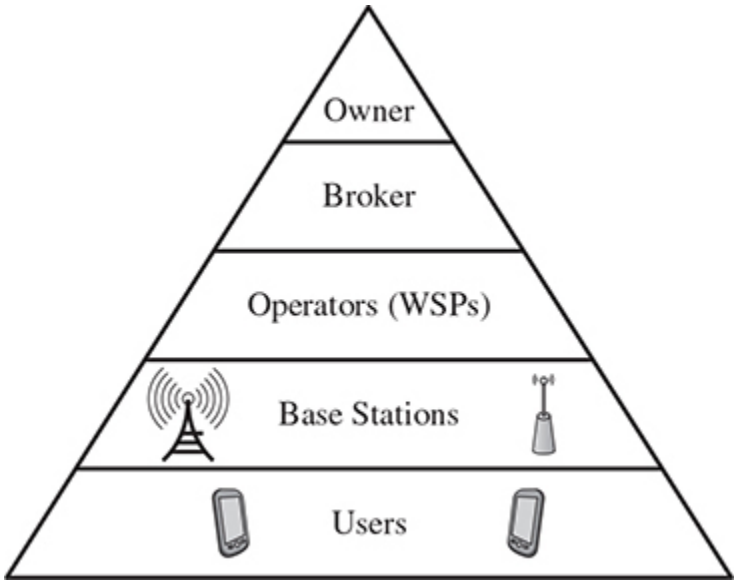


FIGURE 2.1 A spectrum pyramid that represents an architecture for the underutilized spectrum assignments.

2.2.2 Spectrum Auction Model

Consider a spectrum auction setting, where one auctioneer (i.e., the broker in Figure 2.1) auctions a set of frequency bands $\mathcal{M}$ = {1,2,..., M} to $\mathcal{N}$ = {1,2,., N} bidders (i.e., nodes representing BSs) located in the same geographical region where $\mathcal{N}$ represents a set of all bidders that belong to different WSPs. Let *L* be the number of WSPs where each WSP has a coverage area within the auction's geographical region. Each WSP (i.e., the *Ith* WSP) provides a mobile wireless service over multiple cellular cells. Its cellular network consists of macro cells and small cells. Within the coverage area of some macro cells, there exist one or more small cells with pico/femto BSs, see Figure 2.2. Let $\mathcal{N}^1$be the set of all of macro cells and small cells BSs that belong to the *Ith* WSP and let $\mathcal{N}$ be a set of all BSs that belong to the *L* WSPs where $\mathcal{N} = \mathcal{N}^1 \cup \mathcal{N}^2 \cup ... \cup \mathcal{N}^L$ and $\mathcal{N} = |\mathcal{N}|$.

We consider a multiband spectrum auction where each BS can bid for a single or multiple frequency bands from the set of available frequency bands $\mathcal{M}$ based on its demand. Once the broker leases the spectrum owner's unused frequency bands in $\mathcal{M}$ for a time duration *T*, the broker becomes the owner of the spectrum bands in $\mathcal{M}$. Meanwhile, the interested BSs submit their bids to the broker. Let the allocation set $\mathcal{K}$ = {α^1, α^2,...} denotes the set of all possible allocations of the frequency bands $\mathcal{M}$. For example, given that $\mathcal{M}$ = {1,2} and $\mathcal{N}$ = {1,2}, we have $\mathcal{K}$ = {α^1 = ({1,2},{}), α^2 = ({1},{2}), α^3 = ({2},{1}), α^4 = ({},{1,2})}, where (α^1 = ({1, 2}, {}) denotes that frequency bands 1 and 2 are allocated to bidder 1 and nothing to bidder 2. Each BS submits its sealed bids $\mathbf{b_n}$ = [$b_n(\alpha^1)$, $b_n(\alpha^2)$,...], for example, **bi** = [2,1,1,0] indicates that BS 1 bids 2 for allocation α^1,1 for allocation α^2, 1 for allocation α^3, and 0 for allocation α^4. For certain allocation α, the nth BS has a true evaluation value $v_n(\alpha)$. Let $\mathbf{v_n}$ = [$v_n(\alpha^1)$, $v_n(\alpha^2)$,...] be the true evaluation vector for BS n. Let p_n represent the price that is charged by the auctioneer to BS $\mathcal{N}$ for allocating the frequency bands. The utility of BS *n*, denoted by U_n, is defined as the difference between the BS's true evaluation value and the actual price it pays to the auctioneer p_n, $U_n = v_n(\alpha) - p_n$, for a specific allocation a. The auctioneer's revenue from the spectrum sales is defined as $R = \sum_{n=1}^{n=N} p_n$ We assume that BSs can submit different bids for different combinations of the frequency bands. Table 2.1 summarizes some of the notations used in the design.

$\mathcal{M}$	Frequency bands set
$\mathcal{N}^l$	Set of all BSs that belong to WSP l
$\mathcal{N}$	Set of all BSs that belong to the L WSPs, $\mathcal{N} = \mathcal{N}^1 \cup \mathcal{N}^2 \cup \ldots \cup \mathcal{N}^L$
$\mathcal{K}$	Allocation set $\mathcal{K} = \{\alpha^1, \alpha^2, \ldots\}$
$\mathbf{b_n}$	BS n sealed bids vector for the allocation set $\mathcal{K}$
$\mathbf{v_n}$	True evaluation vector of BS n
p_n	Price charged by the auctioneer to BS n
U_n	BS n utility, $U_n = v_n(\alpha) - p_n$
R	Auctioneer's revenue, $R = \sum_{n=1}^{n=N} p_n$

TABLE 2.1 Key Symbols in This Chapter

Figure 2.2 shows two WSPs (i.e., $L = 2$) providing service in the same geographical region where the broker performs its spectrum auction. Both WSPs are interested in the auctioneer's frequency bands $\mathcal{M}$. Therefore, both of them participate in the spectrum auction. In the coverage area of each WSP there exist multiple macro cells and small cells managed by that WSP. BSs requesting additional frequency bands submit sealed bidding vectors to the auctioneer via an intermediate secure gateway to participate in the auction of the underutilized federal spectrum bands. Considering the frequency reuse property [32,43], each BS has certain coverage radius (i.e., assume it is equivalent to the cell's radius). Within the coverage radius of the nth BS, none of the interfering BSs can simultaneously use any of the frequency bands that the nth BS is using. However, a noninterfering BS can use the same frequency band that is simultaneously used by a BS located outside its coverage radius without causing interference, that is, frequency reuse is utilized in our model. The auctioneer constructs an interference conflict graph for all the BSs that are participating in the auction. Figure 2.3 shows the frequency conflict graph with all bidders/BSs that belong to the two WSPs; each BS is connected with other BSs located within its coverage radius (i.e., BS n is connected with all BSs that must not simultaneously use same frequency bands due to interference between them) where the edges represent mutual interference between the corresponding BSs. The interference conflict graph can be constructed using physical or protocol channel model [221, 222]. It is assumed that there exists a pilot channel,

like the one in [83], to exchange information between the auctioneer and the BSs or simply by sending that unsecured information with the bids. Furthermore, the proposed spectrum auction is executed in one subnet after another where a subnet is defined to be a group of BSs that includes one root BS, that is, BS n, and all other BSs that are connected to it through interference edges (i.e., the BSs that have mutual interference with BS n), but not previously considered root BSs. Figure 2.3 shows two subnets in the frequency conflict graph of the two WSPs. Figure 2.4 shows the spectrum auction model for **MTSSA** for two WSPs' participating in the spectrum auction. First, all BSs submit their encrypted bidding vectors via an intermediate gateway that is operated by federal government. The auctioneer then carries out a secure spectrum auction in one subnet after another. It then allocates the winning BSs frequency bands and charges them for the allocated resources.

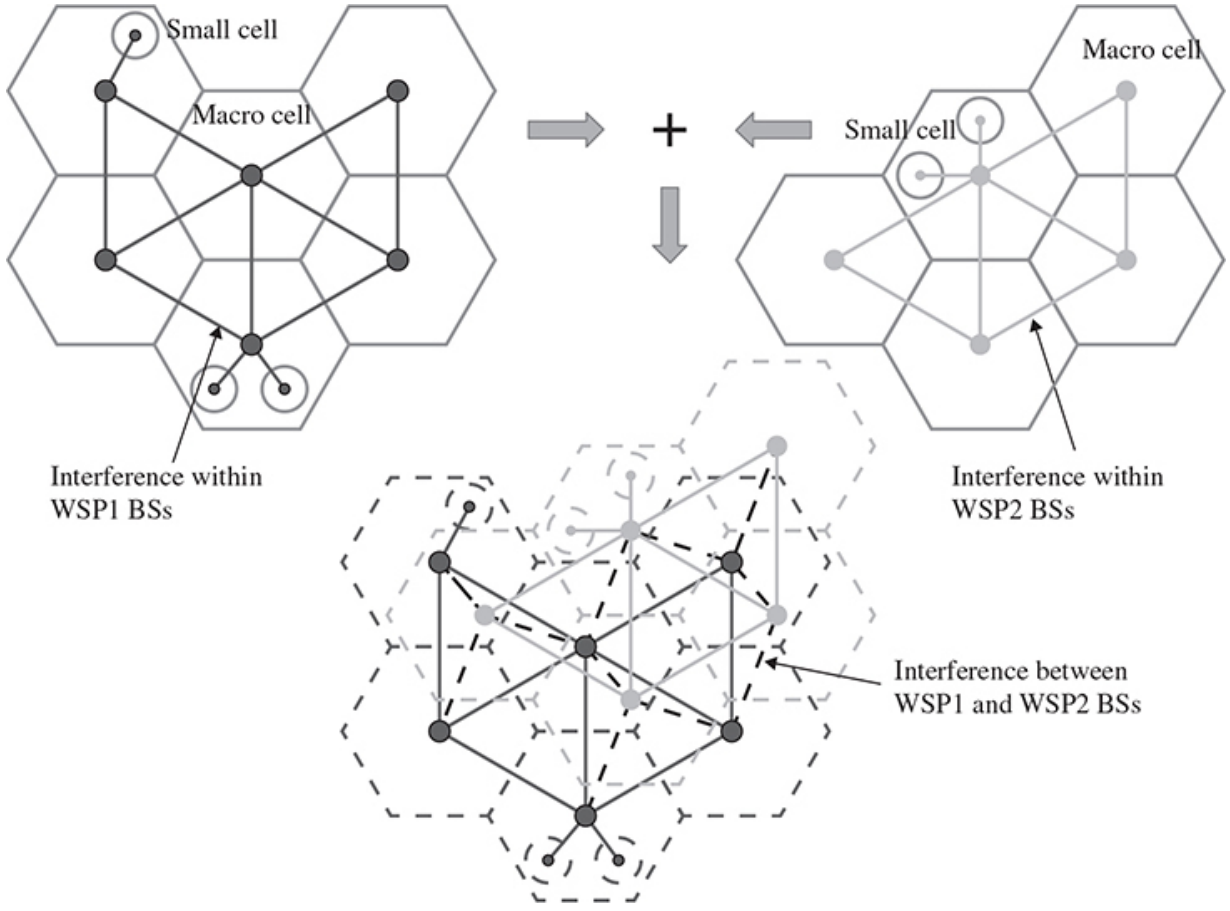


FIGURE 2.2 Two WSPs with a coverage area within the geographical region where the auction takes place. In each WSP's macro cells and small cells,

all the BSs that are interested in the auctioneer's underutilized frequency bands are part of the interference conflict graph.

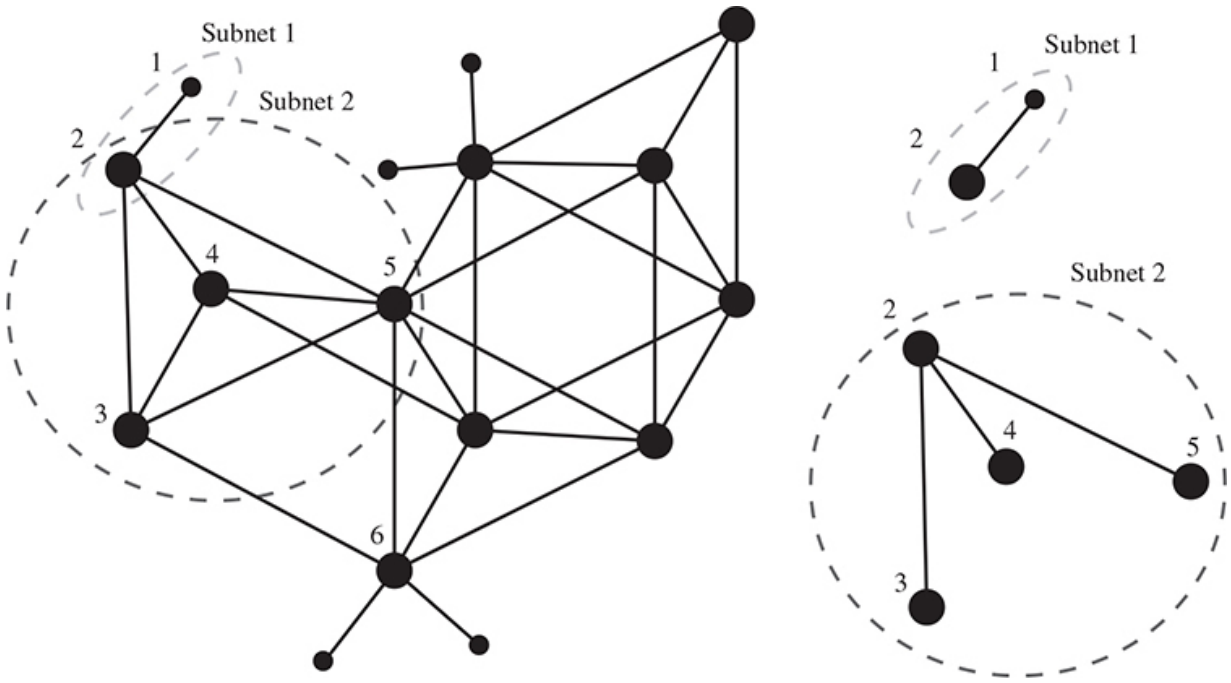


FIGURE 2.3 Frequency conflict graph for all BSs that belong to the two WSPs shown in Figure 2.2. Each node represents one BS and the edges represent mutual interference between the end points (i.e., BSs). Subnet 1 consists of the small cell's BS (i.e., BS 1), which represents the root BS for the subnet, and the macro cell's BS (i.e., BS 2). Subnet 2 consists of BSs 2, 3, 4, and 5 where BS 2 is the root BS.

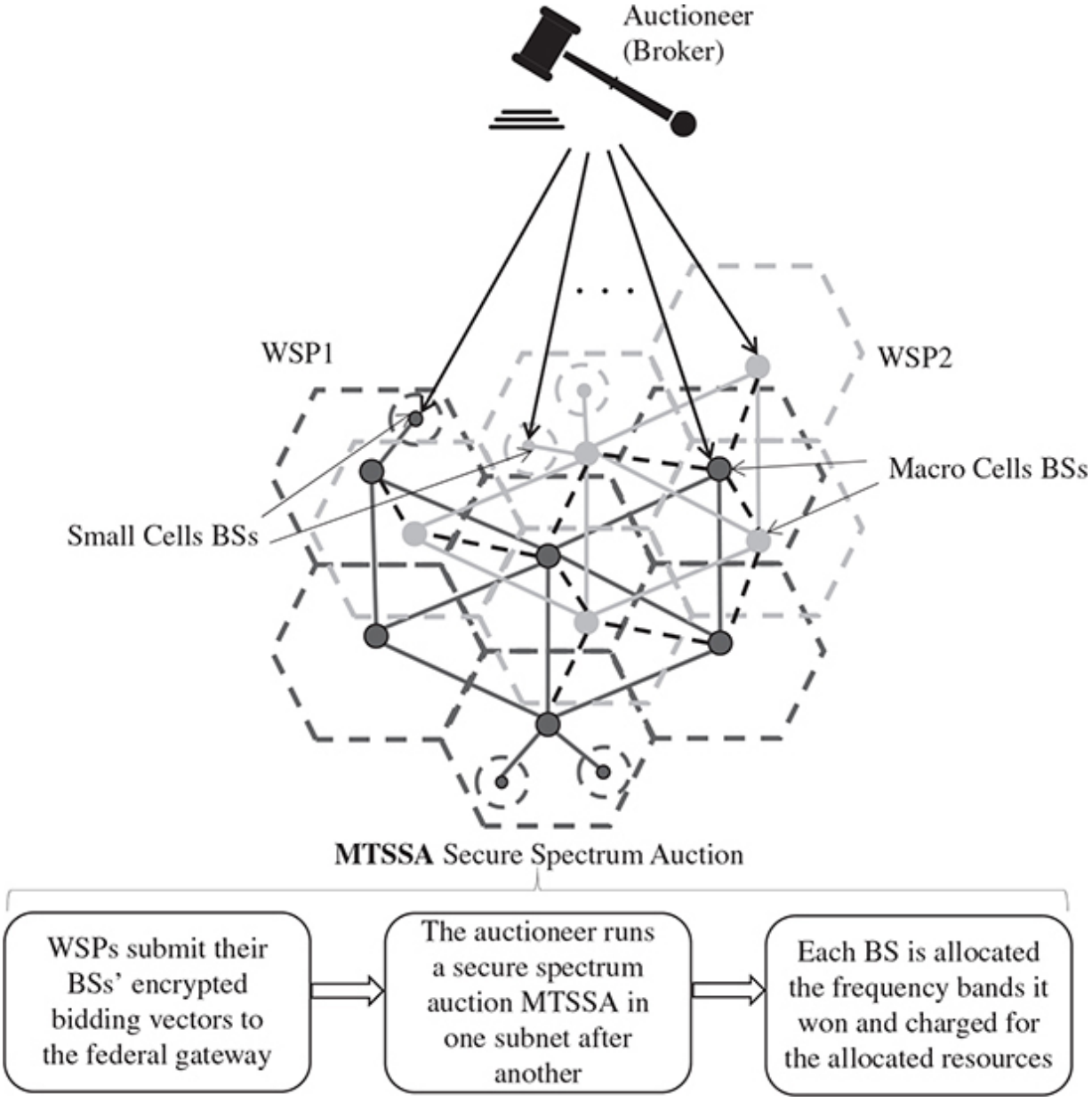

Auctioneer
(Broker)
WSP1
WSP2
Macro Cells BSs
Small Cells BSs
MTSSA Secure Spectrum Auction
WSPs submit their BSs' encrypted bidding vectors to the federal gateway
The auctioneer runs a secure spectrum auction MTSSA in one subnet after another
Each BS is allocated the frequency bands it won and charged for the allocated resources

FIGURE 2.4 Spectrum auction model for the proposed **MTSSA** with two WSPs' BSs participating in the auction.

2.3 Design Considerations

In this section, we present the payment method for the proposed auction. We also discuss some economic properties that need to be considered in the design and prove that by using a VCG-based auction approach some desired economic properties can be satisfied.

2.3.1 The Payment Method

Our goal is to use a payment rule that satisfies some of the required economic properties, such as incentive compatibility, individual rationality, and no positive transfers. In addition, it is important for the payment rule to provide a satisfactory revenue for the auctioneer. Under certain assumptions, it has been proven that VCG auction satisfies these three economic properties while maximizing the auctioneer's revenue [223]. The VCG auction is also proven to be Pareto efficient [224]. In VCG, each bidder submits its true evaluation values regardless of the bidding values that other bidders submit. This is a dominant strategy for the bidder to maximize its utility and win the auction. In our design, we use a payment method that is based on VCG mechanism with Clarke pivot payments [225]. Using this payment rule, each bidder pays the difference between the social welfare with and without his participation (i.e., bidder $\mathcal{N}$ pays the externality he causes). Consider the same system setup as described in Section 2.2. Each BS $\mathcal{N}$ submits its sealed bidding vector $\mathbf{b_n}$ for the allocation set K. The auctioneer selects a Pareto efficient allocation $\alpha^* \in \mathcal{K}$, where α^* is defined as

$$\alpha^* = \arg\max_{\alpha \in \mathcal{K}} \sum_{n} b_n(\alpha) \tag{2.1}$$

With truthful bidding values, the auctioneer assigns its frequency bands $\mathcal{M}$ based on α^* allocation. Furthermore, let $a_{\_n} \in \mathcal{K}$ be an allocation without BS n participating that is defined as

$$\alpha^*_{-n} = \arg\max_{\alpha \in \mathcal{K}} \sum_{k \neq n} b_k(\alpha) \tag{2.2}$$

The auctioneer charges BS n a payment p_n that is equivalent to

$$p_n = \sum_{k \neq n} b_k\left(\alpha^*_{-n}\right) - \sum_{k \neq n} b_k(\alpha^*) \tag{2.3}$$

Then, the utility of BS n can be expressed as

$$
\begin{aligned}
U_n &= v_n(\alpha^*) - p_n \\
&= v_n(\alpha^*) - \left(\sum_{k \neq n} b_k\left(\alpha^*_{-n}\right) - \sum_{k \neq n} b_k(\alpha^*) \right) \\
&= \left[v_n(\alpha^*) + \sum_{k \neq n} b_k(\alpha^*) \right] - \sum_{k \neq n} b_k\left(\alpha^*_{-n}\right)
\end{aligned}
\tag{2.4}
$$

2.3.2 Desired Economic Auction Properties

It is essential for an auction to have certain economic properties. First, we discuss these economic properties and then we prove that by using a VCG-based auction approach these properties can be satisfied.

1. Incentive Compatibility (truthfulness): An auction is incentive compatible if none of the bidders can get higher utility by not reporting its true evaluation vector. Based on this property, a dominant strategy for any bidder is to declare its true evaluation value regardless of what the other bidders do.
2. Individual Rationality: An auction is individually rational if the utility U_n for each bidder n is greater than or equal to zero (i.e., $U_n > 0$). Meaning that the winning bidders obtain non-negative utility (i.e., bidders do not pay more than their evaluation values) from the auction and no one suffers as a result of participating in the auction.
3. No Positive Transfers: In auctions with no positive transfers, the payment of any bidder n must be greater than or equal to zero (i.e., $p_n > 0$). This prevents situations when the auctioneer has to pay the bidders.

Lemmas 2.3.1 to 2.3.3 show that by using the payment method and the VCG-based auction approach discussed above, the aforementioned desired economic properties can be satisfied.

Lemma 2.3.1 Let $\mathbf{v_n}$ and $\mathbf{v'_n} \neq \mathbf{v_n}$ be the nth BS bidding vector when it is equivalent to its true evaluation values and any other values, respectively, and let α^* and $\alpha^{*\prime}$ be the allocations that maximize the social welfare when $\mathbf{v'_n}$ and **vn** are declared, respectively. Then, for the nth BS, the utility $U_n \geq U'_n$.

Proof Using the utility definition and payment method in Section 2.3.1, the utility of BS *n* is $U_n = v_n(\alpha^*) + \sum_{k \neq n} v_k(\alpha^*) - \sum_{k \neq n} v_k(\alpha^*_{-n})$ when declaring **vn,** whereas the utility of BS *n* is $U'_n = v_n(\alpha^{*\prime}) + \sum_{k \neq n} v_k(\alpha^{*\prime}) - \sum_{k \neq n} v_k(\alpha^*_{-n})$ when declaring $\mathbf{V'_n}$. Since α^* is the allocation that maximizes the social welfare, we have the following inequality:

$$\sum_n v_n(\alpha^*) \geq \sum_n v_n(\alpha^{*\prime}) \tag{2.5}$$

Now, by subtracting the term $\sum_{k \neq n} v_k(\alpha^*_{-n})$ from both sides of Equation (2.5), we get $U_n \geq U'_n$, which is the incentive compatibility property.

Lemma 2.3.2 Let α^* and α^*_{-n} be the allocations that maximize the social welfare with and without BS n's participation, respectively, with the assumption that each BS submits its true evaluation values. Then each BS *n* does not suffer as a result of participating in the auction and the auction's winners do not pay more than their evaluation values (i.e., $U_n \geq 0$).

Proof To show individual rationality, consider the utility of BS n:

$$\begin{aligned} U_n &= v_n(\alpha^*) + \sum_{k \neq n} v_k(\alpha^*) - \sum_{k \neq n} v_k\left(\alpha^*_{-n}\right) \\ &\geq \sum_j v_j(\alpha^*) - \sum_j v_j\left(\alpha^*_{-n}\right) \\ &\geq 0 \end{aligned}$$

The first inequality holds since $v_n(\alpha^*) + \sum_{k \neq n} v_k(\alpha^*) \alpha \sum_j {}^{v}i(\alpha^*), \sum_j V_j(\alpha_{-n}) > \sum k \neq_n v_k(\alpha_{-n})$, and $\sum_j v](\alpha_{-n}) > 0$. The second inequality holds because α^* is the allocation that maximizes the social welfare, $\sum_j v_j(\alpha^*)$.

Lemma 2.3.3 As a result of using the payment method in Section 2.3.1, the auction has no positive transfers (i.e., $p_n \geq 0 \; \forall n \in \mathcal{N}$).

Proof From Equation (2.3), we have $p_n = \sum_{k \neq n} b_k(\alpha^*_{-n}) - \sum_{k \neq n} b_k(\alpha^*) \geq 0$, since α^*_{-n} is the allocation that maximizes the social welfare without the $\sum_{k \neq n} b_k(\alpha^*_{-n})$

2.3.3 Design Challenges

Truthfulness is one of the important properties that needs to be taken into consideration when designing a spectrum auction. Sealed secondary price auction and VCG auction are very preferable as they guarantee that bidders submit their true evaluation values. As mentioned earlier, VCG auction has many properties that are essential to have in a spectrum auction. However, VCG requires finding an optimal allocation, which is NP-complete because of the spectrum spatial reusability property. In addition, VCG is vulnerable to frauds of the auctioneer and bid-rigging between the insincere auctioneer and greedy bidders [126]. Therefore, VCG auction cannot be used in a spectrum auction without countermeasures for fraud and bid-rigging.

Bid-rigging between a greedy bidder and an auctioneer can occur for the benefit of both. Since the auctioneer is aware of all bidders' bidding values, he can collude with a greedy bidder and reveal the winning bid value to him. Figure 2.5 shows an example of a spectrum auction where the auctioneer auctions one frequency band $|M| = 1$ to four BSs (i.e., subnet 2 of the frequency conflict graph that is shown in Figure 2.3). The auctioneer runs a VCG auction that is equivalent to a sealed secondary price auction for one frequency band auction. Figure 2.5(α) shows an example of bid-rigging. Bidder 4 is the winner and bidder 2 is a greedy bidder who colludes with the auctioneer and learns about the highest bid. As a result, bidder 2 bids a value that is higher than his true evaluation but a little bit less than the highest bid. By doing so, the auctioneer considers the bidding value of bidder 2 to be the charging price for the winner (i.e., bidder 4). By such a bid-rigging action, the auctioneer can make more profit and share the spoils with bidder 2.

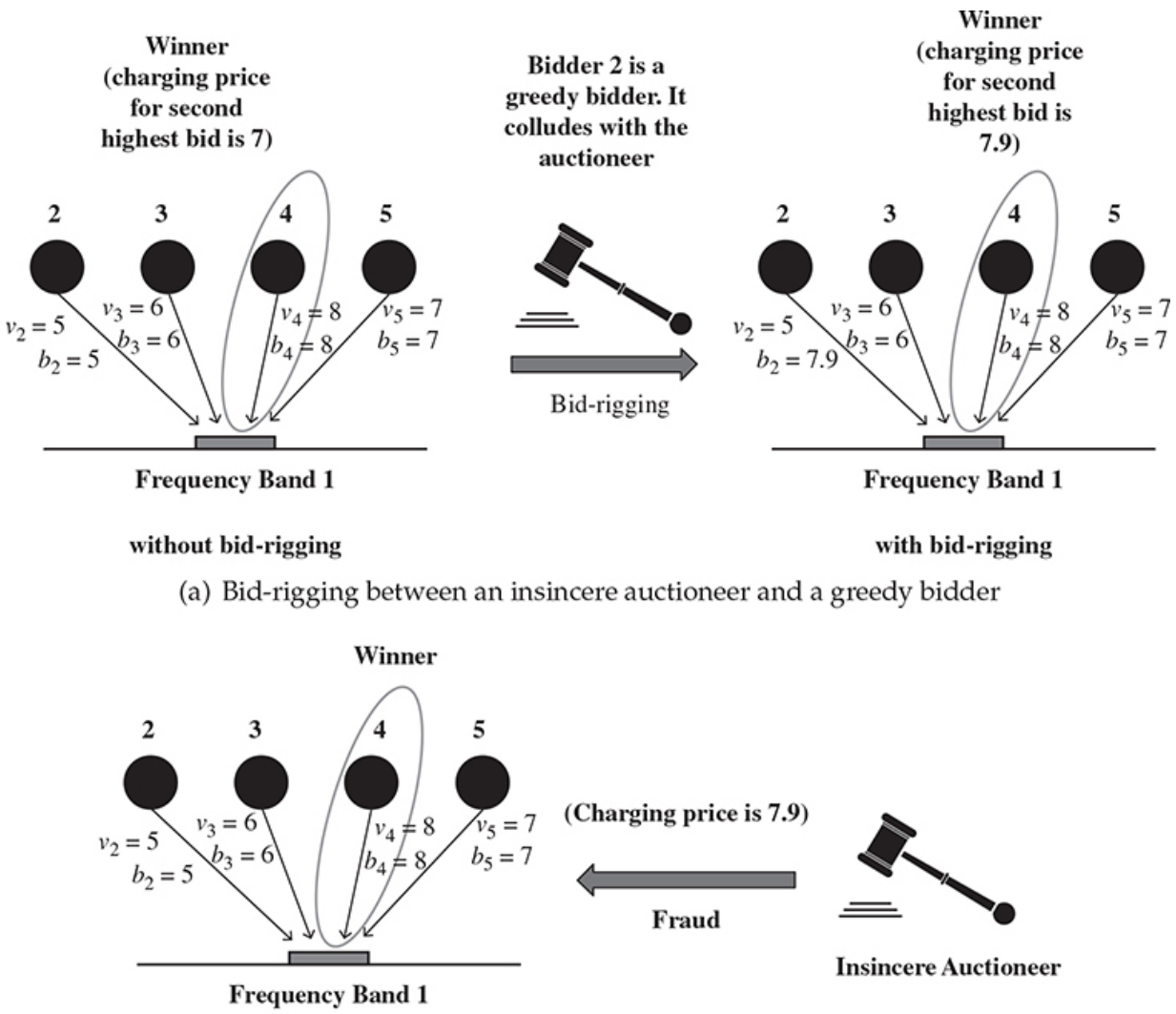


FIGURE 2.5 Examples of bid-rigging and frauds in an unsecured spectrum auction of one frequency band and four BSs.

On the other hand, a fraud occurs when an insincere auctioneer overcharges the winner in order to increase his own profit. This results in an unexpected bad utility for the winner. In Figure 2.5(b), bidder 4 is the winner and the charging price should be 7, which is equivalent to the second highest bid. However, the insincere auctioneer charges bidder 4 at 7.9 to obtain higher revenue. This is possible since all bidding values are sealed and bidders do not know about the bidding values of each other.

To avoid possible bid-rigging and frauds, a successful spectrum auction design needs to take into consideration securing the auction by making the

auctioneer able to decide how to allocate the frequency bands while keeping the bidders' actual bidding values unknown to the auctioneer. This is essential to avoid possible backroom dealing and ensure a secure spectrum auction.

2.4 MTSSA: Secure Spectrum Auction Design

In order to enable an efficient usage of the underutilized shared spectrum managed by a broker. It is important to design a secure spectrum auction that allows the broker to provide a sufficient level of security, privacy, and obfuscation to enable a reliable and efficient usage of the shared spectrum. In order to thwart backroom dealing, it is essential to have a mechanism that allows the auctioneer to find the maximum bid among all bidders without knowing their actual bids. The proposed **MTSSA** leverages Paillier cryptosystem to avoid possible frauds and bid-rigging. In this section, we first describe Paillier cryptosystem and point out its special features. We then discuss **MTSSA** frequency bands allocation procedure. Finally, we present the security part of **MTSSA.**

2.4.1 Paillier Cryptosystem

Some of Paillier cryptosystem properties are essential for our secure spectrum auction design. Paillier cryptosystem [126, 212, 213] is a probabilistic public key encryption system, that is, the term probabilistic encryption indicates that when encrypting the same plaintext for multiple times it yields different ciphertexts that satisfies special features such as homomorphic addition, indistinguishabil-ity, and self blinding.

The homomorphic properties of Paillier cryptosystem provide it with a notable feature. The encryption function of a message $\mathcal{M}$ is given by *C(m)*, is ad-ditively homomorphic, that is, $C(m_1 + m_2) = C(m_1)C(m_2)$. On the other hand, with the indistinguishability property of Paillier cryptosystem, if the plaintext *m* is encrypted twice, the two created cyphertexts are different from each other and no one can distinguish the original plaintexts, except by random guessing, unless decrypting the original ciphertexts. The self-blinding property allows changing the ciphertext publicly without affecting the plaintext. Therefore, from the ciphertext *C(m),* it is possible to compute a different randomized ciphertext *C'(m)* without knowing the decryption

key or the original plaintext.

2.4.2 Frequency Bands Allocation Procedure

All BSs that are interested in the auction and belong to the WSPs within the geographical region of the auction submit their bidding values to participate in the auction. Based on the location of these BSs and which WSPs they belong to, the auctioneer creates an interference conflict graph (i.e., like the one in Figure 2.3). The auctioneer executes the auction in one subnet at a time. For each subnet, the auctioneer selects a random BS $n \in N$ to be the current root BS and considers its corresponding subnet, that is, connected nodes/BSs. After solving for the current subnet, the auctioneer selects a new BS, that has not been a root BS before, to be the new root BS and excludes any previous root BS from its subnet along with the allocated frequency bands to these BSs. Following the same procedure, the auctioneer continues to execute the auction in one subnet after another until each BS has participated in the auction. Based on the subnet auction results, the auctioneer allocates the corresponding root BS the frequency bands and charges it for the allocated resources. Each BS that is participating in the auction maintains a local conflict-table, that is, as in [110].

The **MTSSA** procedure is presented in the following steps:

1. **Each BS $n \in N$ sets up its conflict-table and submits its encrypted version of bidding values $\mathbf{b_n}$:** Each WSP l within the auctioneer's geographical region creates a set of all BSs $\mathcal{N}^1$ that are interested in bidding for the auctioneer's underutilized frequency bands. Each BS $n \in \mathcal{N}^1$ creates a conflict-table with all the interfering BSs denoted by $\mathcal{I}_n$ (i.e., $\mathcal{I}_n$ is a set of all BSs that are located within the coverage area of BS n). Each WSP l provides an update to each BS $n \in \mathcal{N}^1$ regarding its interfering BSs $\mathcal{I}_n$.[2] Each $n \in \mathcal{N}^1$ creates its bidding vector $\mathbf{b_n}$ that will be an input to a buffer that encrypts the bidding values. The encrypted bids are then submitted to federal gateway for randomization, see Section 2.4.3, then sent to auctioneer, see Figure 2.4. Neither the auctioneer nor the other BSs know the actual bidding values $\mathbf{b_n}$ that BS n has submitted. We show in the section "Impact of Paillier Cryptosystem

on the Bidding Values" below the procedure of encrypting the bidding values using Paillier encryption.

2. **Start with a random BS $n \in N$ and consider its corresponding subnet:** The auctioneer does not have an optimal choice regarding which subnet it starts the auction from in order to maximize his revenue. Therefore, the auctioneer selects a random bidder *n* from the set *n* and considers its corresponding subnet (i.e., a subnet consists of a root BS *n* and all other BSs connected to BS *n* in the interference conflict graph except BSs that have been previously considered root BSs).
3. The auctioneer carries out a secure spectrum auction in the subnet of the selected BS ***n:*** The auctioneer performs a secure spectrum auction procedure (detailed in Section 2.4.3) in the current subnet under consideration.
4. **Allocate frequency bands and charge price:** Based on the subnet auction's results, the auctioneer allocates the root BS frequency bands and charges it for the allocated resources. The allocation and the payment vary based on the location of root BS and its relative bid with respect to neighboring BSs. Each winning BS stores its allocated frequency bands and its charging price in the conflict-table.
5. **Proceed to next root BS:** A new root BS is selected based on a random selection done by auctioneer and the corresponding subnet secure bids are sent to auctioneer and the process is repeated starting from Step 2.

Algorithm 1 summarizes **MTSSA** spectrum auction procedure.

2.4.3 Secure Spectrum Auction Using Paillier Cryptosystem

In order for **MTSSA** to ensure a secure auction, it is important to design **MTSSA** such that there is no way for the auctioneer to manipulate the auction. VCG auction is proven to have the incentive compatibility property from the bidders side, which is essential for our design. In order for **MTSSA** to prevent the auctioneer from conducting any frauds or bid-rigging [126], it is important to limit the auctioneer's capability by making

him only able to exploit the winners and their payments without knowing the actual bidding values. So, by leveraging Paillier cryptosystem in our design, **MTSSA** can ensure a secure spectrum auction. Next we discuss in detail how both the BSs and the auctioneer need to collaborate in order to carry out a secure spectrum auction.

Impact of Paillier Cryptosystem on the Bidding Values

Encrypting the Bidding Values Each BS submits its bidding values through a buffer that uses Paillier cyptosystem to encrypt the bidding values and create a vector of ciphertexts for each bidding value. Let s be a number that any actual bidding value does not exceed, and let $z = b(\alpha)$ be the actual bidding value for allocation α such that $1 \leq z \leq s$. Let the vector of ciphertexts for z be **c**(z) that is given by

Algorithm 1 **MTSSA** Frequency Bands Allocation

$\mathcal{N} = \mathcal{N}^1 \cup \mathcal{N}^2 \ldots \cup \mathcal{N}^L$ {i.e., $\mathcal{N}$ is the set of all BSs in the interference conflict graph}
$\mathcal{N}_0 = \mathcal{N}$
Auctioneer generates his private and public keys of Paillier cryptosystem
Auctioneer sends public key and element x to all BSs via pilot channel
while $\mathcal{N} != \phi$ **do**
  $n = random(\mathcal{N})$ {Auctioneer selects a random BS}
  $\mathcal{N}_n = include\_conflict(n)$ {Auctioneer adds BSs that form the nth subnet from conflict-table of nth BS as root}
  $\mathcal{N}_- = (\mathcal{N}_0 \setminus \mathcal{N}) \cap \mathcal{N}_n$ {$\mathcal{N}_-$ is set of previous root BSs in the nth subnet}
  $\mathcal{N}_n = \mathcal{N}_n \setminus \mathcal{N}_-$ {Auctioneer removes from $\mathcal{N}_n$ previous root BSs}
  $\mathcal{M}_- = include\_alloc(\mathcal{N}_-)$ {$\mathcal{M}_-$ is set of freq. bands allocated to $\mathcal{N}_-$}
  $\mathcal{M}_n = \mathcal{M} \setminus \mathcal{M}_-$ {Auctioneer removes from $\mathcal{M}$ freq. bands allocated to $\mathcal{N}_-$}
  $\mathcal{K}_n = alloc\_vect(\mathcal{N}_n, \mathcal{M}_n)$ {Auctioneer forms allocation vector $\mathcal{K}_n$ and sends to $\mathcal{N}_n$}
  BSs $\in \mathcal{N}_n$ send encrypted bids to federal gateway
  Federal gateway randomizes bids and forwards to auctioneer
  Auctioneer selects the highest allocation α^*
  Auctioneer charges price p_n to BS n
  $\mathcal{N} = \mathcal{N} \setminus \{n\}$
end while

$$\begin{aligned} \mathbf{c}(z) &= (c^1, \ldots, c^s) \\ &= (\underbrace{C(x), \ldots, C(x)}_{z}, \underbrace{C(0), \ldots, C(0)}_{s-z}) \end{aligned} \tag{2.6}$$

where C(x) is the Paillier encryption of the public element x (i.e., $x \neq 0$) and C(0) is the Paillier encryption of 0. As mentioned earlier, C has a self-blinding property, which makes z undeterminable without decrypting the elements in **c**(z).

Selecting the Maximum Bidding Value The auctioneer can determine the BS with the maximum bidding value from the encrypted bidding values without knowing their actual values. Let $\mathbf{c}(z_j) = (c^1_j, \ldots, c^s_j)$ be the encrypted bidding vector of BS n for certain allocation α. First, consider the product of all encrypted bidding vectors for allocation α,

$$\prod_j \mathbf{c}(z_j) = (Q_1, \ldots, Q_s) = \left(\prod_j c^1_j, \ldots, \prod_j c^s_j \right) \tag{2.7}$$

Due to the homomorphic addition property of Paillier cryptosystem, Q_i (i.e., $1 \leq i \leq s$ and $i \neq j$) is equivalent to

$$Q_i = \prod_j c^i_j = C^{\gamma(i)}(x) = C(\gamma(i)x) \tag{2.8}$$

where γ(i) represents the number of values that are greater than or equal to i, that is, $\gamma(i) = |\{j : z) >$ Given that γ(i) monotonically decreases when i increases, one way to find the maximum of these bidding values is to decrypt Q_i and check whether the decrypted value $C^{-1}(Q_i)$ equals 0 or not for i changing from $s \rightarrow 1$. Once the largest i with a decrypted value $C^{-1}(Q_i) \neq 0$ is found, then the maximum bidding value for the allocation α is determined to be i (i.e., $i = \max\{zj\}$).

Randomizing the Encrypted Bidding Values Without knowing z, the federal gateway adds a constant t to the encrypted vector **c**(z) and randomizes the rest of its elements. This results in the following vector

$$\mathbf{c}'(z+t) = \left(\underbrace{C(x), \ldots, C(x)}_{z}, c'_1, \ldots, c'_{s-z} \right) \tag{2.9}$$

where *t* cannot be obtained from either **c**(z) or **c**'(z+t) because of the self-blinding property of Paillier cryptosystem. In addition, *t* cannot be figured out by comparing **c***(z)* and **c**(*z* + *t*) during the shifting and randomizing process.

Securing the MTSSA Subnet Auction

By using Paillier cryptosystem as discussed in the section "Impact of Paillier Cryptosystem on the Bidding Values" above, with encrypted bidding values it is still possible to find the maximum bid and the encrypted bidding vectors are randomized without knowing their actual values. This makes it possible to apply a VCG-based auction in each subnet. As mentioned earlier, the proposed **MTSSA** auction is carried out in one subnet after another. In certain subnets, **MTSSA** auction is performed as follows:

1. The auctioneer generates his private and public keys of Paillier cryptosystem and publishes his public key and element *x* over the pilot channel.
2. Each BS submits its sealed bidding vector $\mathbf{b_n} = \mathbf{v_n}$ (i.e., its true evaluation values since we consider a VCG-based auction). The auctioneer creates representing vectors $\boldsymbol{C_T} = \boldsymbol{C(O)}$, $\boldsymbol{C_1} = \boldsymbol{C(O)}$,..., $\boldsymbol{C_N} = \boldsymbol{C(O)}$, where *N* is the number of bidders (i.e., BSs), the initial $O(\alpha)$ equals 0, and the size of vector ***C*** equals $|\mathcal{K}|$. In order for BS *z* to keep his bidding value *bz* secret, he adds his encrypted bidding value to all of the representing vectors except C_z. Once all BSs are done performing this addition, the auctioneer obtains

$$\mathbf{C}_T = \left(\prod_n \mathbf{c}(b_n(\alpha_1)), \ldots, \prod_n \mathbf{c}(b_n(\alpha_{|\mathcal{K}|})) \right) \tag{2.10}$$

   Due to the homomorphic addition property of Paillier cryptosystem, Equation (2.10) is equivalent to

$$\mathbf{C}_T = \left(\mathbf{c}\left(\sum_n b_n(\alpha_1) \right), \ldots, \mathbf{c}\left(\sum_n b_n(\alpha_{|\mathcal{K}|}) \right) \right) = \mathbf{C}\left(\sum_z b_z \right) \tag{2.11}$$

and

$$\mathbf{C}_z = \mathbf{C}\left(\sum_{n \neq z} b_z\right) \quad 1 \leq z \leq N \tag{2.12}$$

3. Federal gateway adds $\theta(\alpha) = t$ to $\mathbf{C}_T, \mathbf{C}_1, \ldots, \mathbf{C}_N$ to obtain $\mathbf{C}(\sum_n b_n + \theta)$ and $\mathbf{C}(\sum_{n \neq z} b_n + \theta) \forall z$. It sends these randomized encrypted bids to auctioneer.
4. In order for the auctioneer to select an allocation for the current subnet and find its corresponding charging price, it finds the maximum sum value

$$\begin{aligned} g &= \arg\max_{\alpha \in \mathcal{K}} \left(\sum_n b_n(\alpha) + \theta(\alpha)\right) \\ &= \arg\max_{\alpha \in \mathcal{K}} \left(\sum_n b_n(\alpha)\right) + t \end{aligned} \tag{2.13}$$

which can be determined by the auctioneer by taking the product of all the encrypted elements in $\mathbf{C}_T$, that is, as discussed in the section "Impact of Paillier Cryptosystem on the Bidding Values" above, which is equivalent to $\prod_{i=1}^{|\mathcal{K}|} \mathbf{c}(\sum_{n=1}^{N} b_n(\alpha_i) + t)$. The auctioneer determines the maximum element in that product, which is equivalent to *g* in Equation (2.13).

5. For each allocation a, the auctioneer decrypts the gth element of vector $\mathbf{c}(\sum_n b_n(\alpha) + \theta(\alpha))$ in $\mathbf{C}_T$ and finds whether it equals 0 or x. If it equals *x* at allocation α*, then the auctioneer selects *α** to be the allocation that maximizes $\sum_n b_n$ in the current subnet and considers its corresponding BSs.

6. To find the charging price for the root BS, the auctioneer decrypts $\mathbf{c}(\sum_{n\neq z} b_n(\alpha^*) + \theta)$ of $\mathbf{C}_z$ and finds the masked value $(\sum_{n\neq z} b_n(\alpha^*) + \theta)$.
7. The auctioneer then finds the maximum masked bid of the product of the encrypted elements $max_{\alpha\in\mathcal{K}}(\sum_{n\neq z} b_n(\alpha)+t)$, similar to Step 4, which is equivalent to $(\sum_{n\neq z} b_n(\alpha^*_{-z}) + t)$.
8. The auctioneer then finds the charging price for root BS of allocation α^* that is given by

$$p_z = \left(\sum_{n\neq z} b_n(\alpha^*_{-z}) + t\right) - \left(\sum_{n\neq z} b_n(\alpha^*) + t\right) \qquad (2.14)$$

2.5 Numerical Results and Analysis

In this section, we first evaluate the performance of the proposed **MTSSA** spectrum auction and compare it with the performance of other spectrum auction mechanisms. Three performance metrics are considered: spectrum utilization, auctioneer's revenue, and bidders' satisfaction. These are the most important performance metrics that need to be maximized in a successful spectrum auction. In addition, we analyze the security strategy of the proposed secure spectrum auction **MTSSA** that makes it able to avoid possible frauds and bid-
rigging.

2.5.1 Performance Analysis

We consider a spectrum auction hosted by the auctioneer (the broker) in a $A * A$ m^2 square geographical region with two cellular networks located within the same region where the auction takes place. Each cellular network belongs to different WSP, that is, there exist two WSPs $L = 2$ that are interested in participating in the spectrum auction. Each WSP has certain number of BSs, located in macro cells or small cells, that are interested in bidding for the auctioneer's underutilized frequency bands. The BSs are

randomly placed in the auction's geographical area. Suppose that the frequency mutual interference between any two BSs is based on the distance between them. Any two macro cells' BSs located within a distance of 0.4A cannot be allocated the same frequency bands and these BSs are connected together in the frequency conflict graph. Also, any small cell's BS cannot be allocated the same frequency bands of any other BS located within a distance of 0.05A from it. In our simulation setup, bids are selected randomly with bidding per frequency band is monotonically decreasing, that is, BS's bid for first frequency band is higher than second frequency band and BS's bid for second frequency band is higher than third frequency band and so on, see [82,158,159].

Based on the frequency assignment policy, three spectrum auction mechanisms are considered in our simulation as described in the following three cases:

- Case 1: Conventional spectrum leasing **(CSL)** case where the government directly leases the underutilized spectrum to the WSP with highest bid. Once the winning WSP is exclusively assigned all frequency bands, it then allocates these resources internally to its BSs. Other WSPs are deprived from these frequency bands.
- Case 2: **MTSSA** where each WSP directly submits all of its BSs' encrypted bids to the auctioneer. The auctioneer decides the frequency bands allocation to each BS whereas the WSP has no control on the resources allocation process. By using **MTSSA** frequency assignment process, each BS can be allocated any number of frequency bands between zero and all of the auctioneer's underutilized frequency bands.
- Case 3: **MTSSA** with fixed limit **(MTSSA-FL)** is a special case of the proposed **MTSSA** where the frequency bands allocation policy is similar to the proposed **MTSSA** but is restricted in the number of frequency bands that each BS can bid for. Each BS bids for a fixed number of frequency bands and it can be allocated any number of frequency bands between zero and that fixed number of frequency bands it submitted the bids for.

We ran Monte Carlo simulation for the three cases described above, and the results are averaged over 25 independent runs in which the location and

the bidding values of the BSs are generated randomly and the performance metrics are evaluated. We consider the network setup described above with different number of macro cells' and small cells' BSs that belong to the two WSPs. First, we consider 8 BSs, that is, 4 macro cells' BSs and 4 small cells' BSs. Second, we consider 12 BSs, that is, 6 macro cells' BSs and 6 small cells' BSs. Third, we consider 16 BSs, that is, 8 macro cells' BSs and 8 small cells' BSs.

We consider three performance metrics to compare between **CSL, MTSSA,** and **MTSSA-FL.** These performance metrics are:

- Spectrum Utilization: It is represented by the sum of the frequency bands that are allocated by the auctioneer to the winning BSs.
- Auctioneer's Revenue: It is given by the sum of all BSs' payments, that is, $R = \sum_{n=1}^{n=N} p_n$.
- Bidders' Satisfaction: It is represented by the sum of all winning BSs' utilities divided by the sum of all BSs' evaluation values, that is, $\sum_{n \in \mathcal{A}} U_n / \sum_{n \in \mathcal{N}} v_n$ where $\mathcal{A}$ is the set of BSs that are allocated frequency bands (i.e., winning BSs).

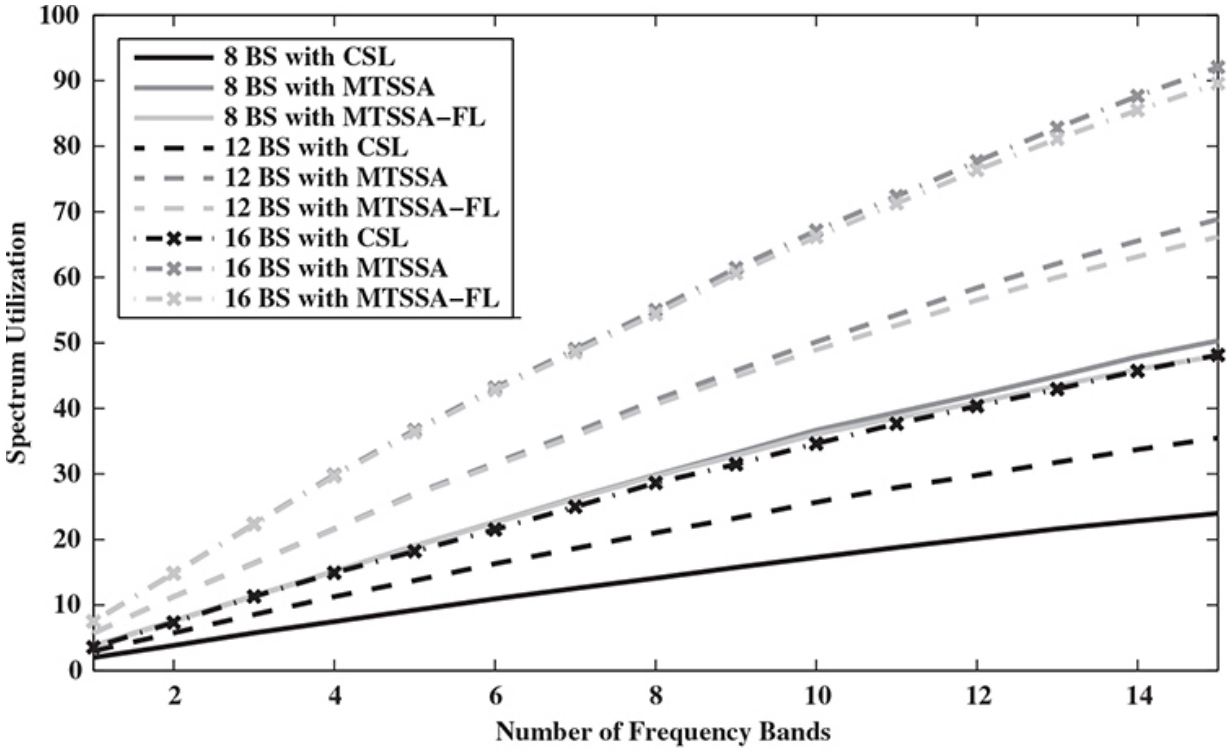
Figure 2.6 compares the performance of the proposed **MTSSA** and its special case **MTSSA-FL** with that of a **CSL**-based auction. We plot the spectrum utilization, auctioneer's revenue, and BSs' satisfaction of the three auction designs with different number of BSs, that is, 8 BSs, 12 BSs, and 16 BSs as mentioned earlier.

Figure 2.6(α) shows the spectrum utilization versus the number of available underutilized frequency bands. As the number of frequency bands increases, the spectrum utilization, which is represented by the number of the allocated frequency bands, also increases for each of the three auction mechanisms. For certain number of frequency bands, each of the three mechanisms shows higher utilization when the number of BSs (bidders) increases. However, it is not surprising that the performance in terms of utilization for **CSL** is lower than that for the other two mechanisms. This is because in **CSL,** the auctioneer assigns each WSP different frequency bands and the frequency bands assigned to each WSP are then auctioned among BSs that belong to that WSP. In the case of **CSL,** the auctioneer considers one frequency conflict graph for each WSP and frequency reusability is not applicable among BSs that belong to different WSPs, that

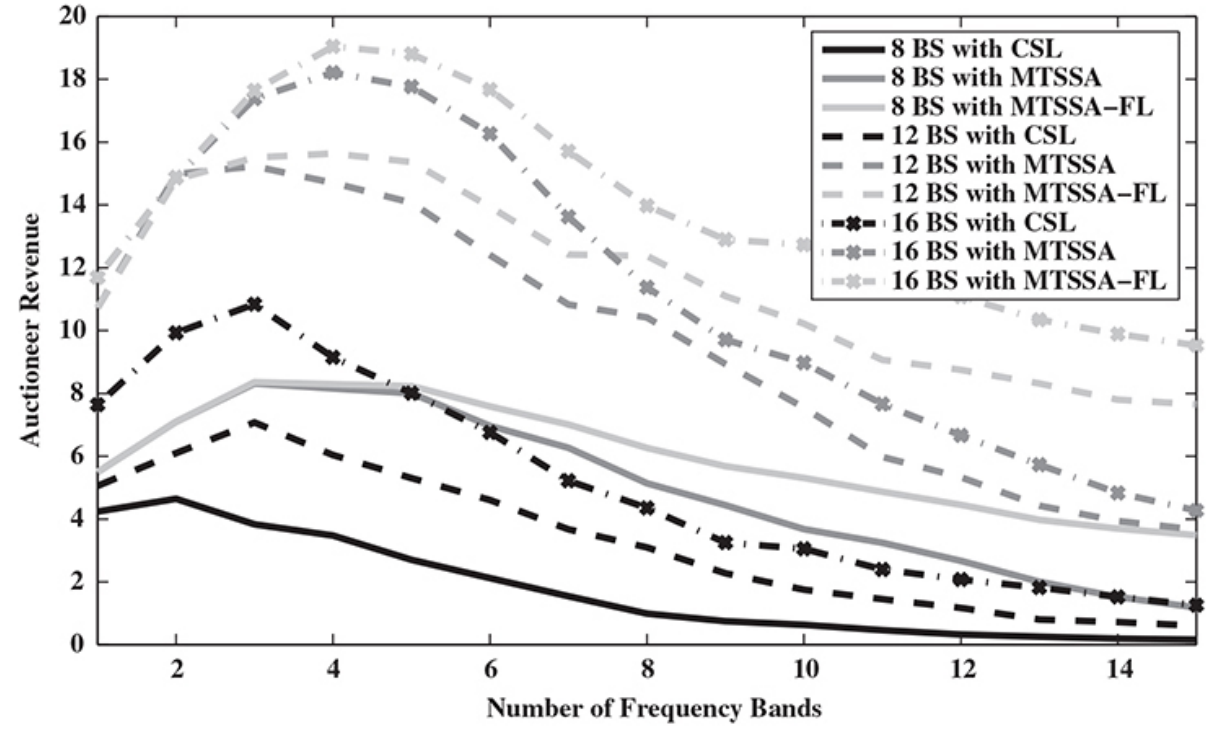
is, BSs that belong to different WSPs and are not within the interference range of each other are not allowed to use the same frequency bands. Moreover, the utilization in the cases of **MTSSA** and **MTSSA-FL** is almost the same when the number of available frequency bands is low and is slightly higher for **MTSSA** than that for **MTSSA-FL** when the number of available frequency bands is higher.

Figure 2.6(b) shows that for each of the three mechanisms, the auctioneer's revenue increases when the number of BSs increases. This is expected as the auctioneer's revenue increases with more bidders requesting more resources. However, for certain number of BSs, the auctioneer's revenue for **MTSSA-FL** is higher than that for **MTSSA** and **CSL,** and as expected the auctioneer's revenue is the lowest in the case of **CSL.** The bump of **MTSSA** over **CSL** is from the payments received from winning BSs that belong to different WSPs, and not located within the interference range of each other, but are allocated similar frequency bands.

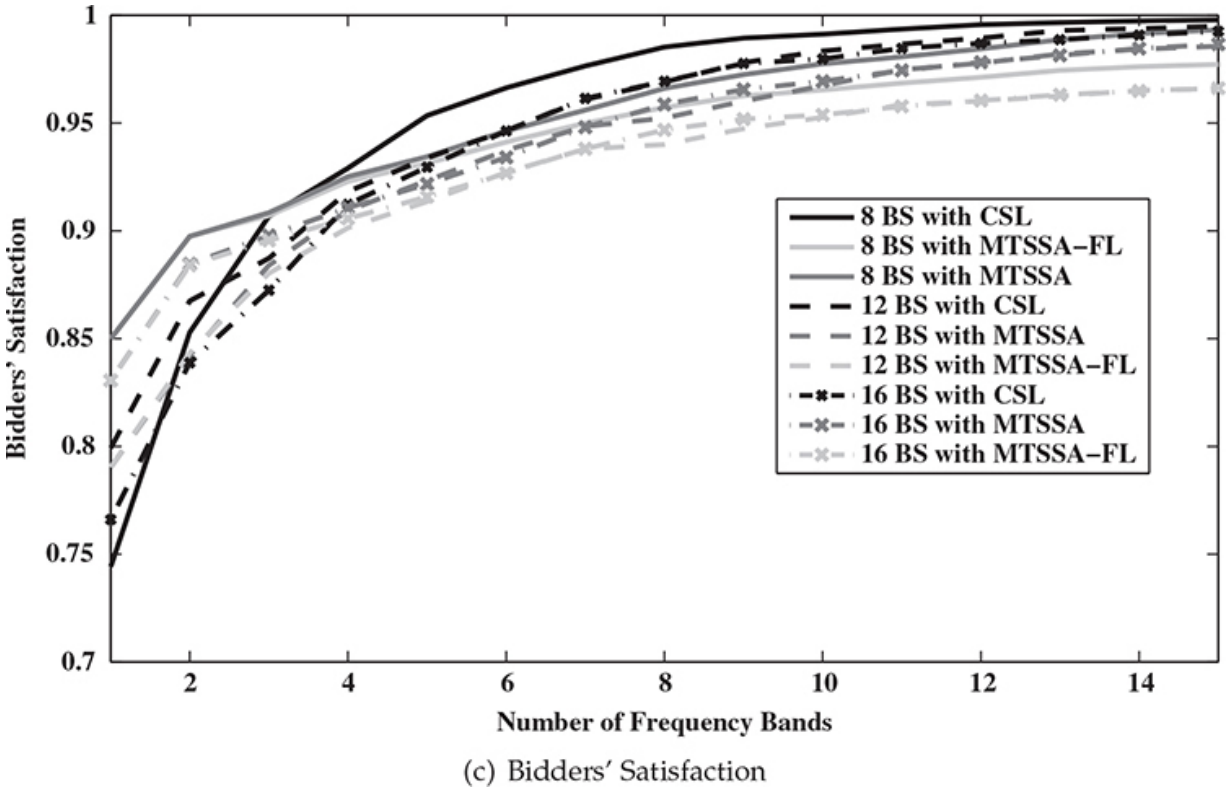
Figure 2.6(c) shows that, as the number of frequency bands increases, the bidders' satisfaction also increases until it saturates when each bidder is allocated the number of frequency bands he bids for. On the other hand, the bidders' satisfaction for **CSL** is higher than that for **MTSSA** and **MTSSA-FL** due to the smaller number of BSs competing for resources as all the frequency bands are allocated to one WSP. Therefore, the bidders who belong to the winning WSP get their requested frequency bands while paying less.



(a) Spectrum Utilization



(b) Auctioneer's Revenue



(c) Bidders' Satisfaction

FIGURE 2.6 Performance comparison of **MTSSA, MTSSA-FL,** and **CSL.**

The comparison between the three mechanisms in Figure 2.6 shows **MTSSA**'s high performance and superiority over **CSL** mechanism as it considers spectrum reusability and in the same time it guarantees a secure spectrum auction.

In addition, we compare the performance of the proposed spectrum auction MTSSA and its ability to maximize the auctioneer's revenue with the spectrum auction mechanism in [116] **(SPRING).** We ran simulations for different numbers of bidders where each bidder is requesting one spectrum at a time by submitting its true evaluation bidding value from the set {1,2,3,4,5}. Simulation results showed that **MTSSA** and **SPRING** achieve almost similar spectrum utilization and bidders' satisfaction when each bidder requests one spectrum band. However, the auctioneer's revenue is much higher in the case of **MTSSA.** This is due to **MTSSA** payment method that is based on VCG auction as well as the spectrum allocation procedure used in **MTSSA,** whereas **SPRING** considers dividing all bidders in groups such that each group contains bidders that do not have mutual frequency interference among them. When running **SPRING,** each

group of bidders submits a bidding value for the whole group that is equivalent to the minimum bidding value among bidders' bids in that group multiplied by the number of bidders in that group. The auctioneer selects the group with the maximum bidding value to be the winner and changes each bidder within that group a price that is equivalent to the minimum bid value in that group. Based on the payment method adopted in **SPRING,** it is obvious that in the case of **MTSSA** spectrum auction, the auctioneer will be gaining more revenue compared to the case when using **SPRING** spectrum auction. Figure 2.7 shows the auctioneer's revenue in the case of **MTSSA** and in the case of **SPRING** for different numbers of bidders. In addition, **MTSSA** prevents possible insincere behavior of the auctioneer or bidders by limiting the auctioneer's capability and making him only able to exploit the winners and their payments without knowing the actual bidding values, whereas, in the case of **SPRING,** the auctioneer is able to determine the value of the minimum bid value which makes fraud of insincere auctioneer possible. Furthermore, **MTSSA** considers the possibility of bidders colluding with each other to manipulate the auction (bid-rigging among bidders) and is designed in a way to avoid these situations whereas bid-rigging among greedy bidders is possible in the case of **SPRING.**

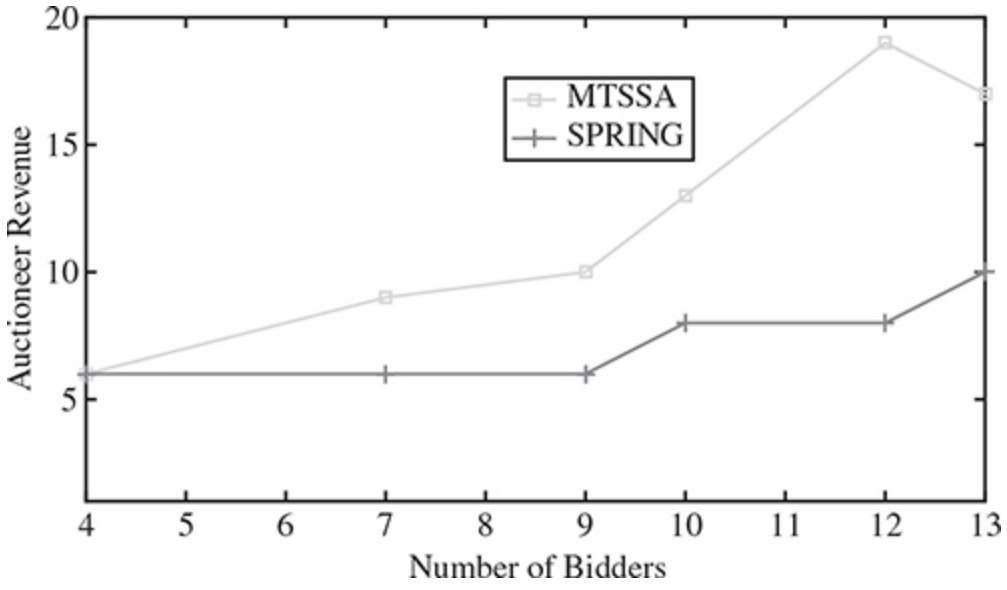


FIGURE 2.7 Comparison between auctioneer's revenue for **MTSSA** and **SPRING.**

2.5.2 MTSSA Security Analysis

As discussed earlier, our proposed **MTSSA** leverages Paillier cryptosystem in order to ensure that the BSs' bidding values are kept unknown to the auctioneer while the auctioneer is still able to find the winners and charges them their corresponding payments. This is possible because of the indistinguishability property of Paillier cryptosystem, that is, it is not possible to know the value of *z* without decrypting each element in c(z), and the self-blinding property that makes it impossible to find a mapping function from c(t) to *C(z* + t) [126, 212, 213]. In order to prevent an insincere auctioneer from performing any frauds, we consider a secure gateway that is operated by federal government. Its main function is to randomize the encrypted bids by the random constant t. So auctioneer can determine the winning allocation and assign secondary price without any knowledge of the original bidding values of BSs. This way **MTSSA** can avoid bid-rigging between an insincere auctioneer and a greedy bidder. This can be guaranteed because even if certain bidder colludes with auctioneer, he cannot find out about the bidding values as federal gateway randomizes it. Therefore, all BSs that belong to different WSPs are treated equally by the proposed **MTSSA** and their bidding values are kept secret from the auctioneer who is only able to determine the winners and their corresponding charged price.

2.5.3 MTSSA Complexity Analysis

In this section, we analyze the computational and communication complexity of **MTSSA** and show its efficiency compared to other secure spectrum auction models such as **THEMIS.** We assume a connected random graph with *n* nodes, so the size of each subnet is in the order of $\mathcal{O}$ (log *N*) [226]. Given the number of spectrum bands available for auction in a subnet to be M, then the number of possible allocations is $\binom{\log N+M-1}{M}$ Using Stirling's formula, we have the number of possible allocations in the order of

$$\mathcal{O}\left(\frac{1}{\sqrt{2\pi M}}\left(1+\frac{M}{\log N-1}\right)^{\log N-\frac{1}{2}}\left(1+\frac{\log N-1}{M}\right)^{M}\right)$$

Table 2.2 shows computational complexity of both **MTSSA** and **THEMIS,** where *s* is the number of possible bidding values. Figure 2.8 plots the upper bounds of the number of possible allocations for **MTSSA** and **THEMIS** using the simulation setup given in Section 2.5. It can be observed that our model computational complexity is more practical and efficient compared to **THEMIS.** For instance, for the allocation of 15 frequency bands in a subnet, **THEMIS** has 10 million possible allocations compared to 100 for **MTSSA.** This explains why authors in [126] have only considered the case when each bidder requests one spectrum band in their simulation results. Similarly, Table 2.3 shows communication complexity of both **MTSSA** and **THEMIS.**

	Computational Complexity
MTSSA	$\mathcal{O}\left(\frac{N\log N}{\sqrt{2\pi M}}\left(1+\frac{M}{\log N-1}\right)^{\log N-\frac{1}{2}}\left(1+\frac{\log N-1}{M}\right)^{M} s\log N\right)$
THEMIS	$\mathcal{O}(N\log N(\log N)^{M} s\log N)$

TABLE 2.2 Computational Complexity Comparison

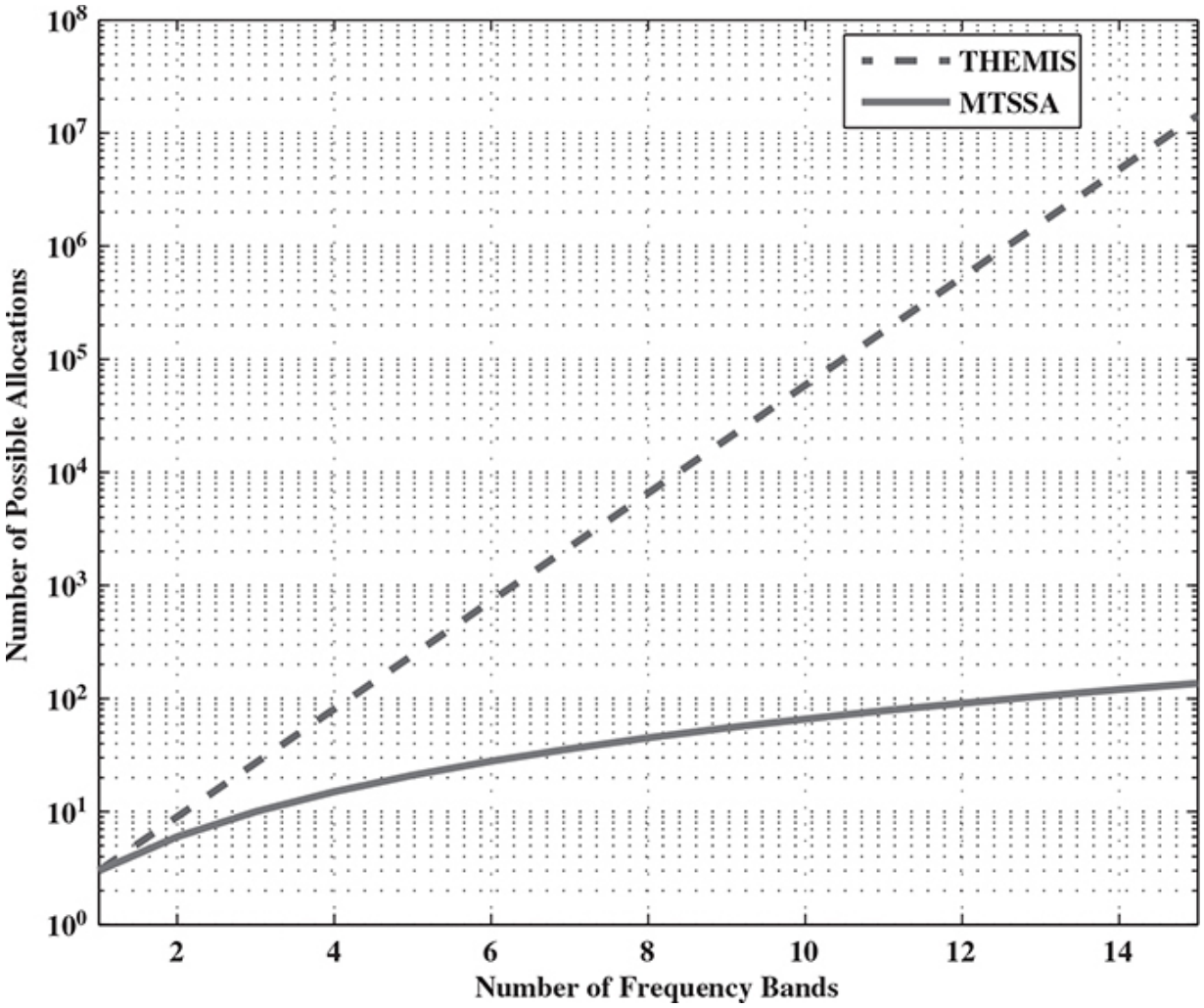


FIGURE 2.8 Comparison between upper bounds of the number of possible allocations for **MTSSA** and **THEMIS.**

	Round	Volume
MTSSA	$\mathcal{O}(N \log N)$	$\mathcal{O}\left(\frac{N \log N}{\sqrt{2\pi M}}\left(1+\frac{M}{\log N-1}\right)^{\log N-\frac{1}{2}}\left(1+\frac{\log N-1}{M}\right)^{M} s \log N\right)$
THEMIS	$\mathcal{O}(N \log N)$	$\mathcal{O}(N \log N(\log N)^{M} s \log N)$

TABLE 2.3 Communication Complexity Comparison

2.6 Conclusion

A secure spectrum auction **MTSSA** is proposed for a multitier dynamic spectrum sharing system. By considering the spectrum reusability property,

MTSSA enables an efficient sharing of the underutilized frequency bands with commercial WSPs. In order to allow spectrum reuse among multiple WSPs, the frequency conflict graph that is considered by **MTSSA** includes all BSs that belong to multiple WSPs and the auction is carried out in one subnet after another. **MTSSA** leverages Paillier cryptosystem and a federal gateway to keep the BSs' bidding values unknown to the auctioneer. The auctioneer uses the additive ho-momorphic property of Paillier cryptosystem to find the winning BSs and their charging prices. This prevents possible frauds and bid-rigging between an insincere auctioneer and greedy BSs. Compared with **CSL** mechanism, **MTSSA** has shown better performance while providing a secure spectrum auction against possible backroom dealings.

---

[1]The content in this chapter is reproduced with permission after modifications (license number 4612590414224). For the original article, refer to [198].

[2]It is assumed that each WSP *l* is aware of all BSs in its coverage area within the auction's geographical region, whether they belong to it or to other WSPs. Therefore, the set of interfering BSs I_n includes all BSs within the coverage area of BS *n* that belong to WSP *l* as well as BSs that belong to other WSPs.

CHAPTER 3

Robust Joint Carrier Aggregation for IoT Spectrum Sharing Systems[1]

Haya Shajaiah, Ahmed Abdelhadi, and Charles Clancy

Spectrum sharing enables wireless systems to harvest underutilized swathes of spectrum, which would vastly increase the efficiency of spectrum usage [228-230]. Making more spectrum available can provide significant gain in mobile broadband capacity only if those resources can be aggregated efficiently with the existing commercial mobile system resources [231-233]. In this chapter, we introduce a resource allocation (RA) based on a carrier aggregation (CA) approach to allocate the network permanent spectrum resources as well as its underutilized spectrum resources based on CA. We present a robust optimal RA with a joint CA approach to allocate multiple carriers' resources optimally among users with elastic and inelastic traffic in cellular networks. We use utility proportional fairness allocation policy, where the fairness among users is in utility percentage of the application running on the user equipment (UE) [234-236]. We introduce an efficient RA approach to allocate the network spectrum resources from multiple carriers based on a CA scenario. We present a robust RA algorithm that allocates optimal aggregated rates for both high-traffic and low-traffic situations. Our distributed RA algorithm allocates an optimal rate to each user from all carriers in its range while providing the minimum price for the allocated rate. In addition, we analyze the convergence of the algorithm with different network traffic densities and show that our algorithm provides traffic-dependent pricing for network providers.

3.1 Introduction

In this chapter, we focus on solving the problem of utility proportional fairness optimal RA with joint CA for multicarrier cellular networks. The RA with joint CA algorithm presented in [91] does not converge for high-traffic situations due to the fluctuation in the RA process. In this chapter, we present a robust algorithm that solves the drawbacks in [91] and allocates multiple carriers' resources optimally among UEs in their coverage area for both high-traffic and low-traffic situations. Additionally, our proposed distributed algorithm outperforms the multistage RA with CA algorithms presented in [237, 238] as it guarantees that mobile users are assigned optimal (minimum) price for resources. We formulate the multicarrier RA with CA optimization problem into a convex optimization framework [239, 240]. We use logarithmic and sigmoidal-like utility functions to represent delay-tolerant and real-time applications, respectively, running on mobile users' smart phones [158]. Our model supports both contiguous and noncontiguous CA from one or more network providers. During the RA process, our distributed algorithm allocates optimal resources from one or more carriers to provide the lowest resource price for the mobile users. In addition, we use a utility proportional fairness approach that ensures nonzero RA for all users and gives real-time applications priority over delay-tolerant applications due to the nature of their applications that require minimum encoding rates.

Our contributions in this chapter are summarized as follows:

- We consider the RA optimization problem with joint CA presented in [91] that uses utility proportional fairness approach and solves for logarithmic and sigmoidal-like utility functions representing delay-tolerant and real-time applications, respectively.
- We prove that the optimization problem is convex and therefore the global optimal solution is tractable. In addition, we present a robust distributed RA algorithm to solve the optimization problem and provide optimal rates in high-traffic and low-traffic situations.
- Our proposed algorithm outperforms that presented in [91] by preventing the fluctuations in the RA process when the resources are scarce with respect to the number of users. It also outperforms the

algorithms presented in [82-84] as it guarantees that mobile users receive optimal price for resources.

- We present simulation results for the performance of our RA algorithm and compare it with the performance of the multistage RA algorithm presented in [82-84].

3.2 Problem Formulation

We consider a long-term evolution (LTE) mobile system consisting of *K* eNodeBs with *K* cells and *M* UEs distributed in these cells. We assume that each cell has one eNodeB with resources that belong to certain carrier and each eNodeB is located in the middle of the cellular cell. Joint UEs are the UEs located under the coverage area of more than one eNodeB and these will be served from all of their in range carriers. We assume that eNodeBs located in cells that do not intersect with each others may have same carrier resources and frequency reuse is applied in this case. The rate allocated by the *Ith* carrier eNodeB to z*i*th UE is given by r_{li}, where $l = \{1,2,..., K\}$ and $i = \{1,2,...,M\}$. Each UE has its own utility function $U_i(r_{1i} + r_2 i + ... + r_{Ki})$ that corresponds to the type of traffic being handled by the *i*th UE. Our objective is to determine the optimal rates that the *Ith* carrier eNodeB should allocate to the nearby UEs. We express the user satisfaction with its provided service using utility functions that represent the degree of satisfaction of the user function with the rate allocated by the cellular network [241-244]. We assume the utility functions $U_i(r_{1i} + r_{2i} + ... + r_{Ki})$ to be a strictly concave or a sigmoidal-like functions. The utility functions have the following properties:

- $U_i(0) = 0$ and $U_i(r_{1i} + r_{2i} + ... + r_{Ki})$ is an increasing function of *ru* for l.
- $U_i(r_{1i} + r_{2i} + .+ r_{Ki})$ is twice continuously differentiable in rj_i for all l.

In our model, we use the normalized sigmoidal-like utility function, as in [245247], that can be expressed as

$$U_i(r_{1i} + r_{2i} + \ldots + r_{Ki}) = c_i \left(\frac{1}{1 + e^{-a_i \left(\sum_{l=1}^{K} r_{li} - b_i \right)}} - d_i \right) \qquad (3.1)$$

where $c_i = \frac{1+e^{a_i b_i}}{e^{a_i b_i}}$ and $d_i = \frac{1}{1+e^{a_i b_i}}$. So, it satisfies $U_i(0) = 0$ and $U_i(\infty) = 1$. We use the normalized logarithmic utility function, as in [248-250], that can be expressed as

$$U_i(r_{1i} + r_{2i} + \ldots + r_{Ki}) = \frac{\log\left(1 + k_i \sum_{l=1}^{K} r_{li}\right)}{\log\left(1 + k_i r_{\max}\right)} \tag{3.2}$$

where $r_{\max}$ is the required rate for the user to achieve 100% utility percentage and k_i is the rate of increase in utility percentage with allocated rates. So, it satisfies $U_i(0) = 0$ and $U_i(r_{\max}) = 1$. We consider the utility proportional fairness objective function that is given by

$$\max_{\mathbf{r}} \prod_{i=1}^{M} U_i(r_{1i} + r_{2i} + \ldots + r_{Ki}) \tag{3.3}$$

where $\mathbf{r} = \{\mathbf{r_u}, \mathbf{r_2}, \ldots, \mathbf{r_M}\}$ and $r_i = \{r_{1i}, r_{2i}, \ldots, r_{Ki}\}$. The goal of this RA objective function is to maximize the total system utility while ensuring proportional fairness between utilities (i.e., the product of the utilities of all UEs). This RA objective function inherently guarantees:

- Nonzero RA for all users. Therefore, the corresponding RA optimization problem provides a minimum quality of service (QoS) for all users.
- Priority to users with real-time applications. Therefore, the corresponding RA optimization problem improves the overall QoS for LTE system.

The basic formulation of the utility proportional fairness RA problem is given by the following optimization problem:

$$
\begin{aligned}
\max_{\mathbf{r}} \quad & \prod_{i=1}^{M} U_i(r_{1i} + r_{2i} + \ldots + r_{Ki}) \\
\text{subject to} \quad & \sum_{i=1}^{M} r_{1i} \le R_1, \sum_{i=1}^{M} r_{2i} \le R_2, \ldots \\
& \ldots \ , \ \sum_{i=1}^{M} r_{Ki} \le R_K, \\
& r_{li} \ge 0, \quad l = 1, 2, \ldots, K, \ \ i = 1, 2, \ldots, M
\end{aligned}
\tag{3.4}
$$

where R_l is the total available rate at the lth carrier eNodeB.

We prove in Section 3.3 that the solution of the optimization problem (3.4) is the global optimal solution.

3.3 The Global Optimal Solution

In the optimization problem (3.4), since the objective function arg $\max_{\mathbf{r}} \prod_{i=1}^{M} U_i(r_{1i} + r_{2i} + \ldots + r_{Ki})$ is equivalent to arg $\max_{\mathbf{r}} \sum_{i=1}^{M} \log(U_i(r_{1i} + r_{2i} + \ldots + r_{Ki}))$, optimization problem (3.4) can be written as:

$$
\begin{aligned}
\max_{\mathbf{r}} \quad & \sum_{i=1}^{M} \log(U_i(r_{1i} + r_{2i} + \ldots + r_{Ki})) \\
\text{subject to} \quad & \sum_{i=1}^{M} r_{1i} \le R_1, \sum_{i=1}^{M} r_{2i} \le R_2, \ldots \\
& \ldots \ , \ \sum_{i=1}^{M} r_{Ki} \le R_K, \\
& r_{li} \ge 0, \quad l = 1, 2, \ldots, K, \ \ i = 1, 2, \ldots, M
\end{aligned}
\tag{3.5}
$$

Lemma 3.3.1 The natural logarithms of utility functions $\log(U_i(r_{1i} + \ldots + r_{Ki}))$ in the optimization problem (3.5) are concave functions.

Proof In Section 3.2, we assume that all the utility functions of the UEs are logarithmic or sigmoidal-like functions. The functions $\log(U_i)$ are concave functions if and only if $-\log(U_i)$ are convex functions. For logarithmic utility functions $U_i(r_{1i} + ... + r_{Ki})$, let $-\log(U_i)$ be denoted by $f(r_{1i}, r_{2i},..., r_{Ki})$, and for sigmoidal-like utility functions $U_i(r_{1i}+ .. .+r_{Ki})$,let $-\log(U_i)$ be denoted by $g(r_{1i}, r_{2i},..., r_{Ki})$. To show that f and g are convex functions, we test for whether the Hessian matrix **H** of each function is positive definite or positive semidefinite. The Hessian matrix of the function $f(r_{1i}, r_{2i},..., r_{Ki})$ is a $K \times K$ symmetric matrix given by

$$\mathbf{H}_f(r_{1i}, r_{2i}, \ldots, r_{Ki}) = \left[\frac{\partial^2 f}{\partial r_{mi}\partial r_{ni}}\right] = \nabla^2 f$$

$$\mathbf{H}_f = \begin{bmatrix} f_{r_{1i}r_{1i}} & f_{r_{1i}r_{2i}} & \cdots & f_{r_{1i}r_{Ki}} \\ f_{r_{2i}r_{1i}} & f_{r_{2i}r_{2i}} & \cdots & f_{r_{2i}r_{Ki}} \\ \vdots & \vdots & \ddots & \vdots \\ f_{r_{Ki}r_{1i}} & f_{r_{Ki}r_{2i}} & \cdots & f_{r_{Ki}r_{Ki}} \end{bmatrix}$$

where $m = \{1, 2, \ldots, K\}, n = \{1, 2, \ldots, K\}$ and $f_{r_{mi}r_{ni}} = \frac{\partial^2 f}{\partial r_{mi}\partial r_{ni}}$ is the element of the mth row and nth column in $\mathbf{H}_f$. The first partial derivative $f_{r_{li}} = \frac{\partial f}{\partial r_{li}}$, where $l = \{1, 2, ... , K\}$, is calculated as follows

$$f_{r_{li}} = \frac{\partial f(r_{1i}, \ldots, r_{Ki})}{\partial r_{li}} = \frac{-k_i}{\log\left(1 + k_i \sum_{l=1}^{K} r_{li}\right)} < 0 \qquad (3.6)$$

and the second partial derivative $fr_{mi}r_{ni}$, that is, $M = \{1,2,...,K\}$ and $N = \{1,2,..., K\}$, is calculated as follows

$$f_{r_{mi}r_{ni}} = \frac{\partial^2 f(r_{1i}, \ldots, r_{Ki})}{\partial r_{li}^2} = \frac{k_i^2}{\left(1 + k_i \sum_{l=1}^{K} r_{li}\right) \log^2 \left(1 + k_i \sum_{l=1}^{K} r_{li}\right)} > 0 \tag{3.7}$$

Let $S_f = \frac{k_i^2}{(1+k_i \sum_{l=1}^{K} r_{li}) \log^2 (1+k_i \sum_{l=1}^{K} r_{li})}$, then it follows that $\mathbf{H}_f$ is equivalent to

$$\mathbf{H}_f = \begin{bmatrix} S_f & \ldots & S_f \\ S_f & \ldots & S_f \\ \vdots & \ddots & \vdots \\ S_f & \ldots & S_f \end{bmatrix}$$

For the $K \times K$ matrix **H,** let a $l \times l$ submatrix of **H** that is formed by deleting $K - l$ columns, that is, columns 1,2,..., K—l,and K—l rows, that is, rows 1,2,..., K—l, from **H** be called the lth-order principal submatrix of **H.** The lth-order principal minor of **H** is equivalent to the determinant of a $l \times l$ principal submatrix.

All first-order principal minors of $\boldsymbol{H}_f$ are equivalent to $|Sf|$, which is greater than zero, that is, $|Sf| > 0$. All lth-order principal minors of $\mathbf{H}_f$, for l = {2,3,..., K}, are equivalent to the determinant of the $l \times l$ submatrix of $\boldsymbol{H}_f$ that is equivalent to

$$\begin{vmatrix} g_{r_{1i}r_{1i}} & g_{r_{1i}r_{2i}} & \cdots & g_{r_{1i}r_{Ki}} \\ g_{r_{2i}r_{1i}} & g_{r_{2i}r_{2i}} & \cdots & g_{r_{2i}r_{Ki}} \\ \vdots & \vdots & \ddots & \vdots \\ g_{r_{Ki}r_{1i}} & g_{r_{Ki}r_{2i}} & \cdots & g_{r_{Ki}r_{Ki}} \end{vmatrix} = 0$$

Since $\mathbf{H}_f$ is a symmetric matrix and every principal minor of $\mathbf{H}_f$ is > 0, it follows that $\mathbf{H}_f$ is positive semidefinite, which implies f is a convex

function. Therefore, the natural logarithms of logarithmic utility functions $\log U_i = —f$ are concave functions.

On the other hand, the Hessian matrix of the function $g(r_{1i}, r_{2i},..., r_{Ki})$ is a $K \times K$ symmetric matrix given by

where $m = \{1, 2, \ldots, K\}$, $n = \{1, 2, \ldots, K\}$, and $g_{r_{mi}r_{ni}} = \frac{\partial^2 g}{\partial r_{mi}\partial r_{ni}}$. The utility function of the normalized sigmoidal-like function is given by Equation (3.1) as $U_i(r_{1i} + r_{2i} + \ldots + r_{Ki}) = c_i(\frac{1}{1+e^{-a_i(\sum_{l=1}^{K} r_{li} - b_i)}} - d_i)$. For $0 < \sum_{l=1}^{K} r_{li} < \sum_{l=1}^{K} R_l$, we have

$$0 < c_i \left(\frac{1}{1 + e^{-a_i\left(\sum_{l=1}^{K} r_{li} - b_i\right)}} - d_i \right) < 1$$

Then

$$0 < 1 - d_i \left(1 + e^{-a_i\left(\sum_{l=1}^{K} r_{li} - b_i\right)} \right) < \frac{1}{1 + c_i d_i}$$

It follows that for $0 < \sum_{l=1}^{K} r_{li} < \sum_{l=1}^{K} R_l$, we have the first and second partial derivatives of the function g as

$$\frac{\partial g(r_{1i},\ldots,r_{Ki})}{\partial r_{li}} = \frac{-a_i d_i e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}}{1-d_i\left(1+e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}\right)} + \frac{-a_i e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}}{\left(1+e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}\right)} < 0$$

$$\frac{\partial^2 g(r_{1i},\ldots,r_{Ki})}{\partial r_{mi}\partial r_{ni}} = \frac{a_i^2 d_i e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}}{c_i\left(1-d_i\left(1+e^{-a\left(\sum_{l=1}^{K} r_{li}-b_i\right)}\right)\right)^2} + \frac{a_i^2 e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}}{\left(1+e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}\right)^2} > 0 = S_g > 0$$

where $l = \{1,2,\ldots, K\}$ and $\frac{\partial^2 g}{\partial r_{mi}\partial r_{ni}}$. is equivalent to $S_g > 0$ for any values of M and n, where $m = \{1,2,., K\}$ and $n = \{1,2,., K\}$. It follows that $\mathbf{H}_g$ is equivalent to

$$\mathbf{H}_g = \begin{bmatrix} S_g & \ldots & S_g \\ S_g & \ldots & S_g \\ \vdots & \ddots & \vdots \\ S_g & \ldots & S_g \end{bmatrix}$$

All first-order principal minors of $\mathbf{H}_g$ are equivalent to $|S_g|$, which is greater than zero, that is, $|S_g| > 0$. All lth-order principal minors of $\mathbf{H}_g$, for $l = \{2,3,\ldots, K\}$, are equivalent to the determinant of the $|X|$ submatrix of $\mathbf{H}_g$ that is equivalent to

$$\begin{vmatrix} S_g & \dots & S_g \\ \vdots & \ddots & \vdots \\ S_g & \dots & S_g \end{vmatrix} = 0$$

Since $\mathbf{H}_g$ is a symmetric matrix and every principal minor of $\mathbf{H}_g$ is ≥ 0, it follows that $\mathbf{H}_g$ is positive semidefinite, which implies g is a convex function. Therefore, the natural logarithm of sigmoidal-like utility functions $\log U_i = —g$ are concave functions.

Therefore, all the utility functions in our model have concave natural logarithms.

Theorem 3.3.2 The optimization problem (3.4) is a convex optimization problem and there exists a unique tractable global optimal solution.

Proof It follows from Lemma 3.3.1 that for all UEs utility functions' natural logarithms are concave functions. Therefore, optimization problem (3.5) is a convex optimization problem [251]. The optimization problem (3.5) is equivalent to optimization problem (3.4); therefore, it is a convex optimization problem. For a convex optimization problem, there exists a unique tractable global optimal
solution [251, 252].

3.4 The Dual Problem

The key to a distributed and decentralized optimal solution of the primal problem in (3.5) is to convert it to the dual problem [131]. The optimization problem (3.5) can be divided into two simpler problems by using the dual problem. We define the Lagrangian as follows

$$
\begin{aligned}
L(\mathbf{r},\mathbf{p}) &= \sum_{i=1}^{M} \log(U_i(r_{1i}+r_{2i}+\ldots+r_{Ki})) \\
&\quad - p_1\left(\sum_{i=1}^{M} r_{1i} + z_1 - R_1\right) - \ldots \\
&\quad - p_K\left(\sum_{i=1}^{M} r_{Ki} + z_K - R_K\right) \\
&= \sum_{i=1}^{M}\left(\log(U_i(r_{1i}+r_{2i}+\ldots+r_{Ki})) - \sum_{l=1}^{K} p_l r_{li}\right) \\
&\quad + \sum_{l=1}^{K} p_l(R_l - z_l) \\
&= \sum_{i=1}^{M} L_i(\mathbf{r}_i,\mathbf{p}) + \sum_{l=1}^{K} p_l(R_l - z_l)
\end{aligned}
\tag{3.8}
$$

where $z_i \geq 0$ is the *Ith* slack variable and p_i is Lagrange multiplier or the shadow price of the ith carrier eNodeB (i.e., the total price per unit rate for all the users in the coverage area of the *l*th carrier eNodeB) and $\mathbf{p} = \{p_1, p_2,..., p_K\}$. Therefore, the *i*th UE bid for rate from the ith carrier eNodeB can be written as $w_{li} = p_l r_{li}$ and we have $\sum_{i=1}^{M} w_{li} = p_l \sum_{i=1}^{M} r_{li}$. The first term in Equation (3.8) is separable in r_i. So we have $\max_{\mathbf{r}} \sum_{i=1}^{M}(\log(U_i(r_{1i}+r_{2i}+\ldots+r_{Ki})) - \sum_{l=1}^{K} p_l r_{li}) = \sum_{i=1}^{M} \max_{\mathbf{r}_i}(\log(U_i(r_{1i}+r_{2i}+\ldots+r_{Ki})) - \sum_{l=1}^{K} p_l r_{li})$. The dual problem objective function can be written as

$$
\begin{aligned}
D(\mathbf{p}) &= \max_{\mathbf{r}} L(\mathbf{r}, \mathbf{p}) \\
&= \sum_{i=1}^{M} \max_{\mathbf{r}_i} (L_i(\mathbf{r}_i, \mathbf{p})) + \sum_{l=1}^{K} p_l (R_l - z_l)
\end{aligned} \tag{3.9}
$$

The dual problem is given by

$$
\begin{aligned}
&\min_{\mathbf{p}} && D(\mathbf{p}) \\
&\text{subject to} && p_l \geq 0, \quad l = 1, 2, \ldots, K.
\end{aligned} \tag{3.10}
$$

So we have

$$
\frac{\partial D(\mathbf{p})}{\partial p_l} = R_l - \sum_{i=1}^{M} r_{li} - z_l = 0 \tag{3.11}
$$

substituting by $\sum_{i=1}^{M} w_{li} = p_l \sum_{i=1}^{M} r_{li}$ we have

$$
p_l = \frac{\sum_{i=1}^{M} w_{li}}{R_l - z_l} \tag{3.12}
$$

Now, we divide the primal problem (3.5) into two simpler optimization problems in the UEs and the eNodeBs. The *i*th UE optimization problem is given by

$$
\begin{aligned}
&\max_{r_i} && \log(U_i(r_{1i} + r_{2i} + \ldots + r_{Ki})) - \sum_{l=1}^{K} p_l r_{li} \\
&\text{subject to} && p_l \geq 0 \\
& && r_{li} \geq 0, \quad i = 1, 2, \ldots, M, l = 1, 2, \ldots, K.
\end{aligned} \tag{3.13}
$$

The second problem is the ith eNodeB optimization problem for rate proportional fairness that is given by

$$\begin{aligned} \min_{p_l} \quad & D(\mathbf{p}) \\ \text{subject to} \quad & p_l \geq 0 \end{aligned} \tag{3.14}$$

The minimization of shadow price p_i is achieved by the minimization of the slack variable z_i ő 0 from Equation (3.12). Therefore, the maximum utility percentage of the ith eNodeB rate r_l is achieved by setting the slack variable $z_l = 0$. In this case, we replace the inequality in primal problem (3.5) constraints by equality constraints and so we have $\sum_{i=1}^{M} w_{li} = p_l R_l$. Therefore, we have $p_l = \frac{\sum_{i=1}^{M} w_{li}}{R_l}$ where $w_{li} = p_l r_{li}$ is transmitted by the *i*th UE to ith eNodeB. The utility proportional fairness in the objective function of the optimization problem (3.4) is guaranteed in the solution of the optimization problems (3.13) and (3.14).

3.5 Distributed Optimization Algorithm

The distributed RA algorithm in [91] for optimization problems (3.13) and (3.14) is an iterative solution for allocating the network resources from multiple carriers simultaneously with utility proportional fairness policy. The algorithm is divided into the *i*th UE algorithm as shown in Algorithm 1 [91] and the ith eNodeB carrier algorithm as shown in Algorithm 2 [91]. In Algorithms 1 and 2 [91], the *i*th UE starts with an initial bid $w_{il}(1)$, which is transmitted to the ith carrier eNodeB. The ith eNodeB calculates the difference between the received bid $w_{li}(n)$and the previously received bid $w_{li}(n — 1)$ and exits if it is less than a prespecified threshold ∞. We set $w_{li}(0) = 0$. If the value is greater than the threshold, the *i*th eNodeB calculates the shadow price $p_l = \frac{\sum_{i=1}^{M} w_{li}}{R_l}$ and sends that value to all UEs in its coverage area. The *i*th UE receives the shadow prices p_l from all in range carriers eNodeBs and compares them to find the first minimum shadow price $p^1{}_{min}(n)$ and the corresponding carrier index $l_1 \in L$, where $L = \{1,2,..., K\}$. The *i*th UE solves for the l_1 carrier rate $r_{l_1 i}(n)$ that maximizes $\log U_i(r_{1i} + \ldots + r_{Ki}) - \sum_{l=1}^{K} p_l(n) r_{li}$ with respect to r_{l1i}. The rate

$r_i^1(n) = r_{l_1 i}(n)$ is used to calculate the new bid $w_{l_1 i}(n) = p^1_{\min}(n) r_i^1(n)$. The *i*th UE sends the value of its new bid $w_{l_1 l}(n)$ to the i_1 carrier eNodeB. Then, the *i*th UE selects the second minimum shadow price $p^2_{min}(n)$ and the corresponding carrier index $l_2 \in L$. The *i*th UE solves for the l_2 carrier rate $r_{l_2 i}(n)$ that maximizes log $U_i(r_{1i} + \ldots + r_{Ki}) - \sum_{l=1}^{K} p_l(n) r_{li}$ with respect to $r_{l_2 i}$. The rate $r_{l_2 i}(n)$ subtracted by the rate from l_1 carrier $r_i^2(n) = r_{l_2 i}(n) - r_i^1(n)$ is used to calculate the new bid $w_{l_2 i}(n) = p^2_{\min}(n) r_i^2(n)$, which is sent to l_2 carrier eNodeB. In general, the *i*th UE selects the mth minimum shadow price $p^m_{\min}(n)$ with carrier index $l_m \in L$ and solves for the l_m carrier rate $r_{l_m i}(n)$ that maximizes log $U_i(r_{1i} + \ldots + r_{Ki}) - \sum_{l=1}^{K} p_l(n) r_{li}$ with respect to $r_{l_m i}$. The rate $r_{l_m i}(n)$ subtracted by l_1, l_2,..., $l_{m\text{-}1}$ carriers rates $r_i^m(n) = r_{l_m i}(n) - (r_i^1(n) + r_i^2(n) + \ldots + r_i^{m-1}(n))$ is used to calculate the new bid $w_{l_m i}(n) = p^m_{\min}(n) r_i^m(n)$, which is sent to l_m carrier eNodeB. This process is repeated until $|w_{li}(n) - w_{li}(n-1)|$ is less than the threshold ∞ for all *l* carriers.

The distributed algorithm in [91] is set to avoid the situation of allocating zero rate to any user (i.e., no user is dropped). This is inherited from the utility proportional fairness policy in the optimization problem, similar to [158], [159], and [160]. In addition, the UE chooses from the nearby carriers eNodeBs the one with the lowest shadow price and starts requesting bandwidth from that carrier eNodeB. If the allocated rate is not enough or the price of the resources increases due to high demand on that carrier eNodeB resources from other UEs, the UE switches to another nearby eNodeB carrier with a lower resource price to be allocated the rest of the required resources. This is done iteratively until an equilibrium between demand and supply of resources is achieved and the optimal rates are allocated in the LTE mobile network. Figure 3.1 shows a block diagram that represents the distributed RA algorithm.

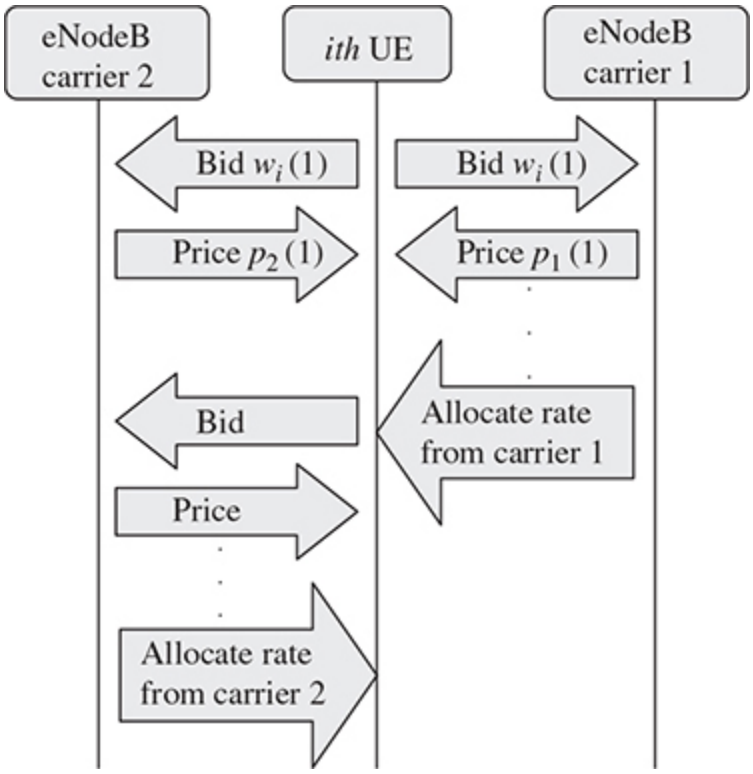


FIGURE 3.1 Flow diagram with the assumption that the shadow price from the first carrier eNodeB p_1 is less before the nith iteration so rate $r\pm;$ of the *ith* user is allocated. After the n_1th iteration, the shadow price from the second carrier eNodeB p_2 is less so rate r_{2i} is allocated.

3.6 Convergence Analysis

In this section, we present the convergence analysis of Algorithms 1 and 2 in [91] for different values of carriers eNodeBs rates *Ri.* This analysis is equivalent to low- and high-traffic hours analysis in cellular systems (e.g., change in the number of active users *M* and their traffic in the cellular system [159]).

3.6.1 Drawbacks of Algorithms 1 and 2

Lemma 3.6.1 For sigmoidal-like utility function $U_i(r_{1i}+r_{2i}+\ldots+r_{Ki})$, the slope curvature function $\frac{\partial \log U_i(r_{1i}+r_{2i}+\ldots+r_{Ki})}{\partial r_{li}}$ has an inflection point at $\sum_{l=1}^{K} r_{li} = r_i^s \approx b_i$ and is convex for $\sum_{l=1}^{K} r_{li} > r_i^s$.

Proof For the sigmoidal-like function $U_i(r_{1i}+r_{2i}+\ldots+r_{Ki}) = c_i(\frac{1}{1+e^{-a_i(\sum_{l=1}^{K} r_{li}-b_i)}} - d_i)$, let $S_i(r_{li}) = \frac{\partial \log U_i(r_{1i}+r_{2i}+\ldots+r_{Ki})}{\partial r_{li}}$ be the slope curvature function. Then, we have that

$$\frac{\partial S_i}{\partial r_{li}} = \frac{-a_i^2 d_i e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}}{c_i\left(1-d_i\left(1+e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}\right)\right)^2} - \frac{a_i^2 e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}}{\left(1+e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}\right)^2}$$

and

$$\frac{\partial^2 S_i}{\partial r_{li}^2} = \frac{a_i^3 d_i e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}\left(1-d_i\left(1-e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}\right)\right)}{c_i\left(1-d_i\left(1+e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}\right)\right)^3} + \frac{a_i^3 e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}\left(1-e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}\right)}{\left(1+e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}\right)^3} \tag{3.15}$$

and

We analyze the curvature of the slope of the natural logarithm of sigmoidal-like utility function. For the first derivative, we have $\frac{\partial S_i}{\partial r_{li}} < 0 \quad \forall\, r_{li}$. The first term $S^1{}_i$ of $\frac{\partial^2 S_i}{\partial r_{li}^2}$ in Equation (3.15) can be written ;

$$S_i^1 = \frac{a_i^3 e^{a_i b_i}\left(e^{a_i b_i} + e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}\right)}{\left(e^{a_i b_i} - e^{-a_i\left(\sum_{l=1}^{K} r_{li}-b_i\right)}\right)^3} \tag{3.16}$$

and we have the following properties:

$$\begin{cases} \lim_{\sum_{l=1}^{K} r_{li} \to 0} S_i^1 = \infty, \\ \lim_{\sum_{l=1}^{K} r_{li} \to b_i} S_i^1 = 0 \text{ for } b_i \gg \frac{1}{a_i} \end{cases} \tag{3.17}$$

For second term S_i^2 of $\frac{\partial^2 S_i}{\partial r_i^2}$ in Equation (3.15), we have the following properties:

$$\begin{cases} S_i^2(r_{li} = b_i - \sum_{j \neq l} r_{ji}) = 0, \\ S_i^2(r_{li} > b_i - \sum_{j \neq l} r_{ji}) > 0, \\ S_i^2(r_{li} < b_i - \sum_{j \neq l} r_{ji}) < 0 \end{cases} \tag{3.18}$$

From Equations (3.17) and (3.18), S_i has an inflection point at $\sum_{l=1}^{K} r_{li} = r_i^s \approx b_i$.In addition, we have the curvature of S_i changes from a convex function close to origin to a concave function before the inflection point $\sum_{i \in \mathcal{M}^l} r_i^{inf} \ll R_l \; \forall \, l \in L$ then to a convex function after the inlection point.

Our rate-allocation approach guarantees nonzero rate allocation for all active users in the coverage area of a specific carrier eNodeB. We define the set $\mathcal{M}^l$:= {i : *rli* ≥ 0} to be the set of active users covered by the *l*th eNodeB. Then, we have the following corollary.

Corollary 3.6.2 If $\sum_{i \in \mathcal{M}^l} r_i^{inf} \ll R_l \; \forall \, l \in L$ then Algorithms 1 and 2 in [91] converge to the global optimal rates, which correspond to the steady state shadow price $\text{price } p_{ss} < \frac{a_{i_{\max}} d_{i_{\max}}}{1 - d_{i_{\max}}} + \frac{a_{i_{\max}}}{2}$, where $i_{\max} = \arg\max_{i \in \mathcal{M}^l} b_i$.

[j]max

Proof For the sigmoidal-like function $U_i(r_{1i} + r_{2i} + \ldots + r_{Ki}) = c_i(\frac{1}{1 + e^{-a_i(\sum_{l=1}^{K} r_{li} - b_i)}} - di)$, the optimal solution is achieved by solving the optimization problem (3.5). In

Algorithm 1 [91], an important step to reach to the optimal solution is to solve the optimization problem $r_{li}(n) = \arg\max_{r_{li}}(\log U_i(r_{1i} + r_{2i} + \ldots + r_{Ki}) - p_l(n)r_{li})$ for every UE in the *i*th eNodeB coverage area. The solution of this problem can be written, using the Lagrange multipliers method, in the form

From Equations (3.17) and (3.18) in Lemma 3.6.1, we have the curvature of $S_i(r_{li})$ is convex for $\sum_{l=1}^{K} r_{li} > r_i^s \approx b_i$. The algorithm in [91] is guaranteed to converge to the global optimal solution when the slope $S_i(r_{li})$ of all the utility functions natural logarithms $\log U_i(r_{1i}+r_{2i}+\ldots+r_{Ki})$ are in the convex region of the functions, similar to the analysis of logarithmic functions in [131] and [133]. Therefore, the natural logarithm of sigmoidal-like functions $\log U_i(r_{1i}+r_{2i}+\ldots+r_{Ki})$ converge to the global optimal solution for $\sum_{l=1}^{K} r_{li} > r_i^s \approx b_i$. The inflection point of sigmoidal-like function $U_i(r_{1i} + r_{2i} + \ldots + r_{Ki})$ is at $r_i^{\inf} = b_i$. For $\sum_{i\in\mathcal{M}^l} r_i^{\inf} \ll R_l$, the algorithm in [91] allocates rates $\sum_{l=1}^{K} r_{li} > b_i$ for all users. Since $S_i(r_{li})$ is convex for $\sum_{l=1}^{K} r_{li} > r_i^s \approx b_i$ then the optimal solution can be achieved by Algorithms 1 and 2 in [91]. We have from Equation (3.19) and as $S_i(r_{li})$ is convex for $\sum_{l=1}^{K} r_{li} > r_i^s \approx b_i$, that $p_{ss} < S_i(\sum_{l=1}^{K} r_{li} = \max_{i\in\mathcal{M}^l} b_i)$, where $S_i(\sum_{l=1}^{K} r_{li} = \max_{i\in\mathcal{M}^l} b_i) = \frac{a_{i_{\max}} d_{i_{\max}}}{1-d_{i_{\max}}} + \frac{a_{i_{\max}}}{2}$ and $i_{\max} = \arg\max_{i\in\mathcal{M}^l} b_i$.

We define the set $\mathcal{M}^{\mathcal{L}} := \{i : r_{li} \neq 0\ \forall\ l \in \mathcal{L}, r_{li} = 0\ \forall\ l \notin \mathcal{L}\}$ to be the set of active users covered exclusively by the set of carriers eNodeBs $U_i(r_{1i} + \ldots + r_{Ki}) - \sum_{l=1}^{K} p_l(n)r_{li}$ Then, we have the following corollary.

Corollary 3.6.3 For $\sum_{i\in\mathcal{M}^{\mathcal{L}}} r_i^{inf} > \sum_{l\in\mathcal{L}} R_l$ and the global optimal shadow price $p_{ss} \approx \frac{a_i d_i e^{\frac{a_i b_i}{2}}}{1-d_i(1+e^{\frac{a_i b_i}{2}})} + \frac{a_i e^{\frac{a_i b_i}{2}}}{(1+e^{\frac{a_i b_i}{2}})}$,, where $i \in \mathcal{M}^{\mathcal{L}}$, then the solution given by Algorithms 1 and 2 in [91] fluctuates about the global optimal rates.

Proof For the sigmoidal-like function $U_i(r_{1i}+r_{2i}+\ldots+r_{Ki}) = c_i(\frac{1}{1+e^{-a_i(\sum_{l=1}^{K} r_{li}-b_i)}} - di)$, it follows from Lemma 3.6.1 that for $\sum_{i\in\mathcal{M}^{\mathcal{L}}} r_i^{\inf} > \sum_{l\in\mathcal{L}} R_l\ \exists\ i \in \mathcal{M}^{\mathcal{L}}$ such such that the optimal rates $\sum_{l=1}^{K} r_{li}^{\text{opt}} < b_i$. Therefore, if

$p_{ss} \approx \frac{a_i d_i e^{\frac{a_i b_i}{2}}}{1-d_i(1+e^{\frac{a_i b_i}{2}})} + \frac{a_i e^{\frac{a_i b_i}{2}}}{(1+e^{\frac{a_i b_i}{2}})}$. is the optimal shadow price for optimization problem (3.5). Then, a small change in the shadow price $p_l(n)$ in the nth iteration can lead the rate $r_{li}(n)$ (root of $S_i(r_{li}) - p_l(n) = 0$) to fluctuate between the concave and convex curvature of the slope curve $S_i(r_{li})$ for the *i*th user. Therefore, it causes fluctuation in the bid $w_{li}(n)$ sent to the eNodeB and fluctuation in the shadow price $p_i(n)$ set by eNodeB. Therefore, the iterative solution of Algorithms 1 and 2 in [91] fluctuates about the global optimal rates $\sum_{l=1}^{K} r_{li}^{\text{opt}}$.

Theorem 3.6.4 Algorithms 1 and 2 in [91] do not converge to the global optimal rates for all values of R_l.

Proof It follows from Corollaries 3.6.2 and 3.6.3 that Algorithms 1 and 2 in [91] do not converge to the global optimal rates for all values of R_1.

3.6.2 Solution Using Algorithms 2 and 3

For a robust algorithm, we add a fluctuation decay function to the algorithm presented in [91] as shown in Algorithm 2. Our robust algorithm ensures convergence for all values of the carriers eNodeBs maximum rate *Ri* for all i. Algorithms 2 and 3 allocated rates coincide with Algorithms 1 and 2 in [91] for $\sum_{i \in \mathcal{M}^l} r_i^{\text{inf}} \ll R_l \ \forall \ l \in L$. For $\sum_{i \in \mathcal{M}^{\mathcal{L}}} r_i^{\text{inf}} > \sum_{l \in \mathcal{L}} R_l$, robust algorithm avoids the fluctuation in the nonconvergent region discussed in the previous section. This is achieved by adding a convergence measure $\Delta w(n)$ that senses the fluctuation in the bid's w_{li}. In case of fluctuation, it decreases the step size between the current and the previous bid $w_{li}(n) - w_{li}(n-1)$ for every user *i* using *fluctuation decay function.* The fluctuation decay function could be in the following forms:

- *Exponentiai function:* It takes the form $\Delta w(n) = h_1 e^{-\frac{n}{h_2}}$

- *Rationai function:* It takes the form $\Delta w(n) = \frac{h_3}{n}$

where h_1,h_2, and h_3 can be adjusted to change the rate of decay of the bid's w_{li}.

Algorithm 2 The ith UE Algorithm

Send initial bid $w_{li}(1)$ to lth carrier eNodeB (where $l \in L = \{1, 2, \ldots, K\}$)
loop
  Receive shadow prices $p_{l \in L}(n)$ from all in range carriers eNodeBs
  if STOP from all in range carriers eNodeBs **then**
    Calculate allocated rates $r_{li}^{\text{opt}} = \frac{w_{li}(n)}{p_l(n)}$
    STOP
  else
    Set $p_{\min}^0 = \{\}$ and $r_i^0 = 0$
    for $m = 1 \rightarrow K$ **do**
      $p_{\min}^m(n) = \min(\mathbf{p} \setminus \{p_{\min}^0, p_{\min}^1, \ldots, p_{\min}^{m-1}\})$
      $l_m = \{l \in L : p_l = \min(\mathbf{p} \setminus \{p_{\min}^0, p_{\min}^1, \ldots, p_{\min}^{m-1}\})\}$ {l_m is the index of the corresponding carrier}
      Solve $r_{l_m i}(n) = \arg\max_{r_{l_m i}} \left(\log U_i(r_{1i} + \ldots + r_{Ki}) - \sum_{l=1}^{K} p_l(n) r_{li} \right)$ for the l_m carrier eNodeB
      $r_i^m(n) = r_{l_m i}(n) - \sum_{j=0}^{m-1} r_i^j(n)$
      if $r_i^m(n) < 0$ **then**
        Set $r_i^m(n) = 0$
      end if
      Calculate new bid $w_{l_m i}(n) = p_{\min}^m(n) r_i^m(n)$
      if $|w_{l_m i}(n) - w_{l_m i}(n-1)| > \Delta w(n)$ **then**
        $w_{l_m i}(n) = w_i(n-1) + \text{sign}(w_{l_m i}(n) - w_{l_m i}(n-1)) \Delta w(n)$ {$\Delta w = h_1 e^{-\frac{n}{h_2}}$ or $\Delta w = \frac{h_3}{n}$}
      end if
      Send new bid $w_{l_m i}(n)$ to l_m carrier eNodeB
    end for
  end if
end loop

Remark 3.6.5 The fluctuation decay function can be included in the UE or the eNodeB algorithm.

In our model, we add the decay part to the UE algorithm as shown in Algorithm 2.

The proposed RA algorithm is a distributed algorithm so an increase in the number of UEs or eNodeBs does not provide a computational burden on the system. In a realistic system, the number of associated eNodeBs with a single UE is limited due to coverage limitations of a single cell and cell planning considerations, which relieve the computational burden on the UE algorithm. The computation complexity of the proposed algorithm is $O((k')^3 \log(\frac{1}{\delta}))$ for k' cells/ eNodeBs and error ∞, where k' here is the maximum number of eNodeBs associated with one UE ($k' \leq K$), which is usually less than K; that is, the worst case is $k' = K$ if all the eNodeBs can cover the same UE, which is not a realistic case.

Algorithm 3 The lth eNodeB Algorithm

loop
  Receive bids $w_{li}(n)$ from UEs {Let $w_{li}(0) = 0 \ \forall i$}
  if $|w_{li}(n) - w_{li}(n-1)| < \delta \ \forall i$ **then**
    Allocate rates, $r_{li}^{\text{opt}} = \frac{w_{li}(n)}{p_l(n)}$ to ith UE
    STOP
  else
    Calculate $p_l(n) = \frac{\sum_{i=1}^{M} w_{li}(n)}{R_l}$
    Send new shadow price $p_l(n)$ to all UEs
  end if
end loop

3.7 Numerical Results

Algorithms 2 and 3 were applied to various logarithmic and sigmoidal-like utility functions with different parameters in MATLAB. The simulation results showed convergence to the global optimal rates. In this section, we present the simulation results for two heterogeneous networks (HetNet)s, where each heterogeneous network consists of macro cells and small cells with the small cells located in the macro cells. The macro cells' eNodeBs are configured at the LTE-Advanced carrier, and the small cells' eNodeBs are configured to use the 3.5-GHz underutilized spectrum band. Each network has a number of active UEs located within the coverage area of its macro cells and small cells. Each UE is running real-time or delay-tolerant applications that are represented by sigmoidal-like functions and logarithmic functions, respectively. We use three normalized sigmoidal-like functions that are expressed by Equation (3.1) with different parameters.

The used parameters are $a = 5$, $b = 10$ (Sig1) corresponding to a sigmoidal-like function that is an approximation to a step function at rate $r = 10$ (e.g., VoIP), $a = 3$, $b = 20$ (Sig2) corresponding to a sigmoidal-like function that is an approximation of an adaptive real-time application with inflection point at rate $r = 20$ (e.g., standard-definition video streaming), and $a = 1$, $b = 30$ (Sig3) corresponding to a sigmoidal-like function that is also an approximation of an adaptive real-time application with inflection point at rate $r = 30$ (e.g., high-definition video streaming), as shown in Figure 3.2. We use three logarithmic functions that are expressed by Equation (3.2) with $r_{\max} = 100$ and different k_i parameters which are approximations for delay-tolerant applications (e.g., FTP). We use $k = 15$ (Log1), $k = 3$ (Log2), and $k = 0.5$ (Log3), as shown in Figure 3.2. The simulation was run using MATLAB in Appendix A.

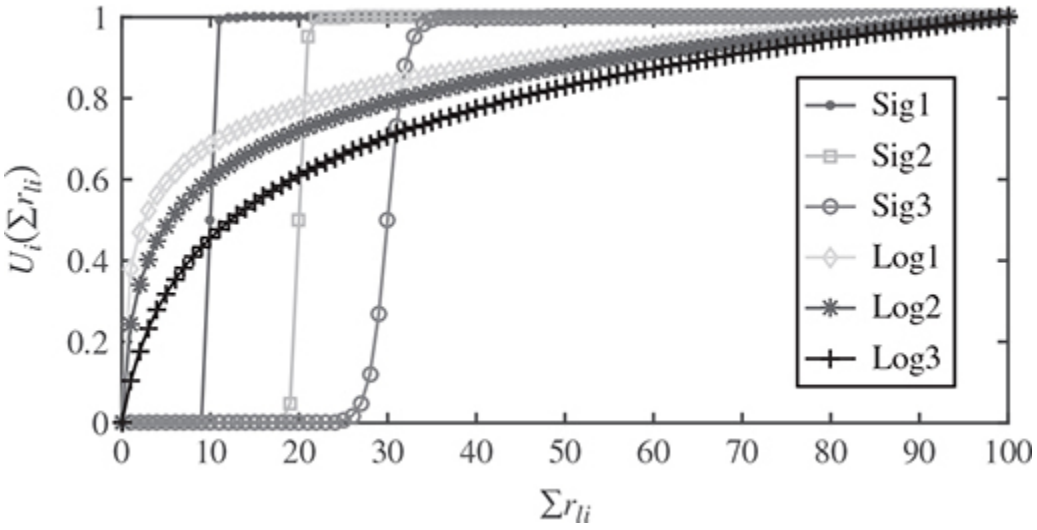


FIGURE 3.2 The users utility functions $U_i(\sum_{l=1}^{K} r_{li})$ used in the simulation (three sigmoidal-like functions and three logarithmic functions).

In Sections 3.7.1 and 3.7.2, we discus the simulation setups for the two heterogeneous networks and discuss the corresponding simulation results.

3.7.1 First Heterogeneous Network

The simulated cellular network in this section is a HetNet (HetNetl) that consists of one macro cell, one small cell, 12 active UEs, and two eNodeBs as shown in Figure 3.3. The UEs are divided into two groups. The 1st group

of UEs (index i = {1,2,3,4,5,6}) is located under the coverage of the macro cell carrier Cl eNodeB, whereas the 2nd group of UEs (index i = {7,8,9,10,11,12} is located in the small cell under the coverage area of both the 1st carrier (C1) and the 2nd carrier (C2) eNodeBs. The maximum achievable rates of C1 and C2 are given by r_1 and r_2, respectively. Each UE is running either real-time or delay-tolerant applications represented by the utility functions shown in Figure 3.2. A three-dimensional view of the sigmoidal-like utility function $U_i(r_{1i} + r_{2i})$ is shown in Figure 3.4. The utility function parameters used to represent the UEs applications for HetNet1 are summarized in Table 3.1.

Allocated Rates in HetNetl for $30 \leq \boldsymbol{R_i} \leq$ **200 and** $\boldsymbol{R_2}$= 70

In the following simulations, we set $\infty = 10^{-3}$, the 1st carrier eNodeB rate r_1 takes values between 30 and 200 with step of 10, and the 2nd carrier eNodeB rate is fixed at r_2 = 70. Figure 3.5 shows the final allocated optimal rates $r_i = r_{1i} + r_{2i}$ of different users with different 1st carrier eNodeB total rate R_1 and observe how the behavior of simulation matches our derived mathematical results due to the consideration of extreme cases, for example, fluctuation in RA in the case of scarce available resources ($R_1 + R_2 < 120$ in this case). Figure 3.5(α) shows the rates allocated to the 1st group of UEs by only C1 eNodeB since C2 eNodeB is not within these users' range, we observe the increase in the rate allocated to these users with the increase in r_1. Figure 3.5(b) shows the final allocated rates to the 2nd group of UEs by both C1 and C2 eNodeBs. Since these users are located under the coverage area of both the macro cell and the small cell, they are allocated rates jointly using the proposed RA with

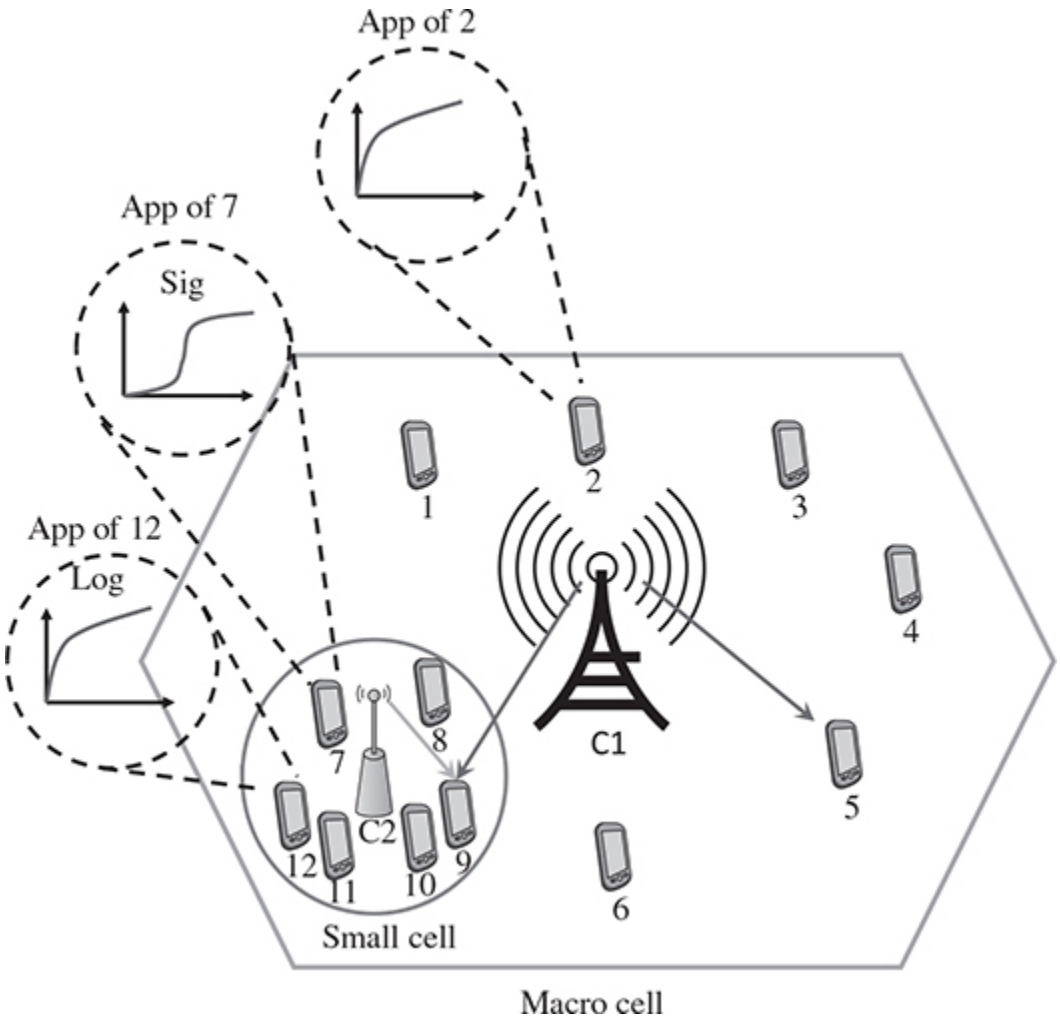


FIGURE 3.3 System model for HetNetl with two groups of users. The 1st group with UE indexes ***i*** = {1, 2,3,4, 5, 6}, 2nd group with UE indexes ***i*** = {7, 8,9,10,11,12}.

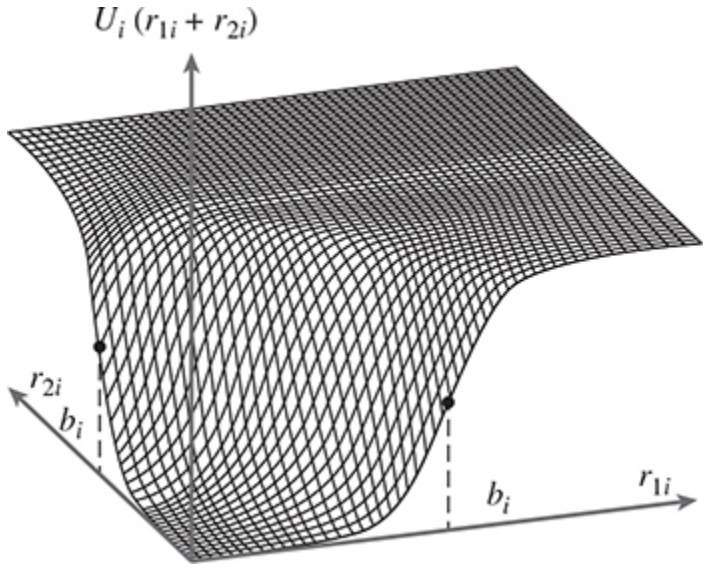
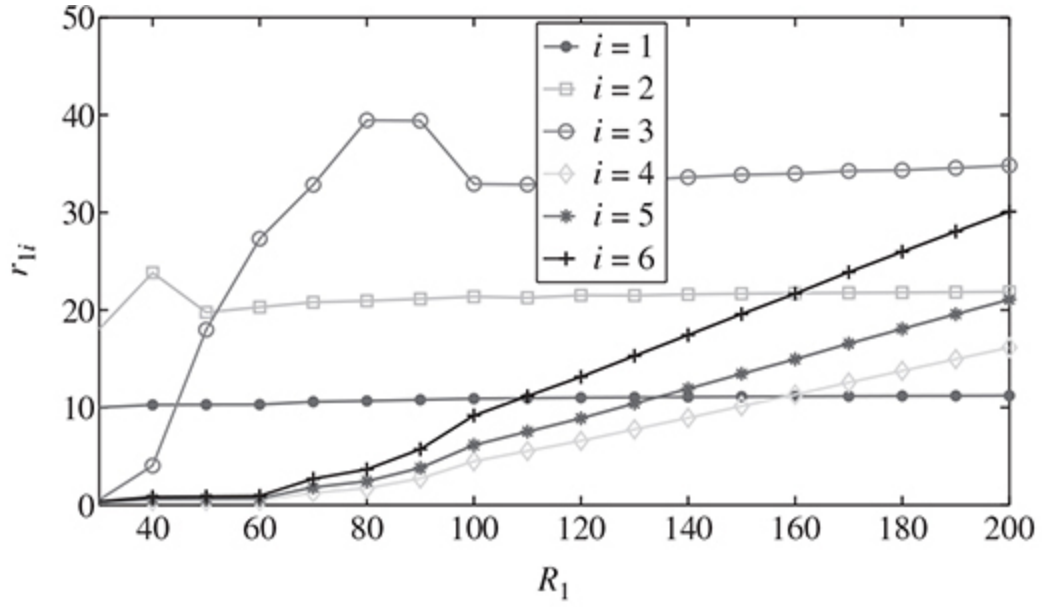


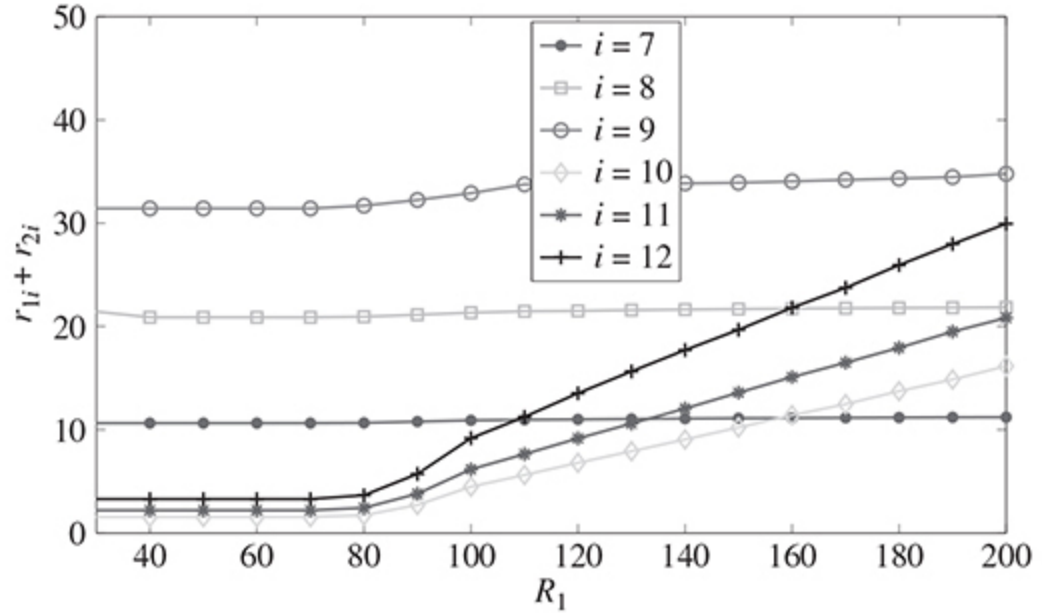
FIGURE 3.4 The sigmoidal-like utility $U_i(r_{1i} + r_{2i}) = c_i(\frac{1}{1+e^{-a_i(r_{1i}+r_{2i}-b_i)}} - d_i)$ of the ***ith*** user in HetNetl, where is the rate allocated by 1st carrier eNodeB and r_{2i} is the rate allocated by 2nd carrier eNodeB. joint CA approach. Figure 3.5(a) and 3.5(b) show that by using the RA with joint CA algorithm, no user is allocated zero rate (i.e., no user is dropped). However, the majority of the eNodeBs resources are allocated to the UEs running adaptive real-time applications until they reach their inflection rates the eNodeBs then allocate more resources to the UEs with delay-tolerant applications, as real-time application users bid higher than delay-tolerant application users by using the utility proportional fairness policy.

Applications Utilities Parameters		Users Indexes
Sig1	Sig $a = 5,\ b = 10$	$i = \{1, 7\}$
Sig2	Sig $a = 3,\ b = 20$	$i = \{2, 8\}$
Sig3	Sig $a = 1,\ b = 30$	$i = \{3, 9\}$
Log1	Log $k = 15,\ r_{max} = 100$	$i = \{4, 10\}$
Log2	Log $k = 3,\ r_{max} = 100$	$i = \{5, 11\}$
Log3	Log $k = 0.5,\ r_{max} = 100$	$i = \{6, 12\}$

TABLE 3.1 Users and Their Applications Utilities in HetNet1



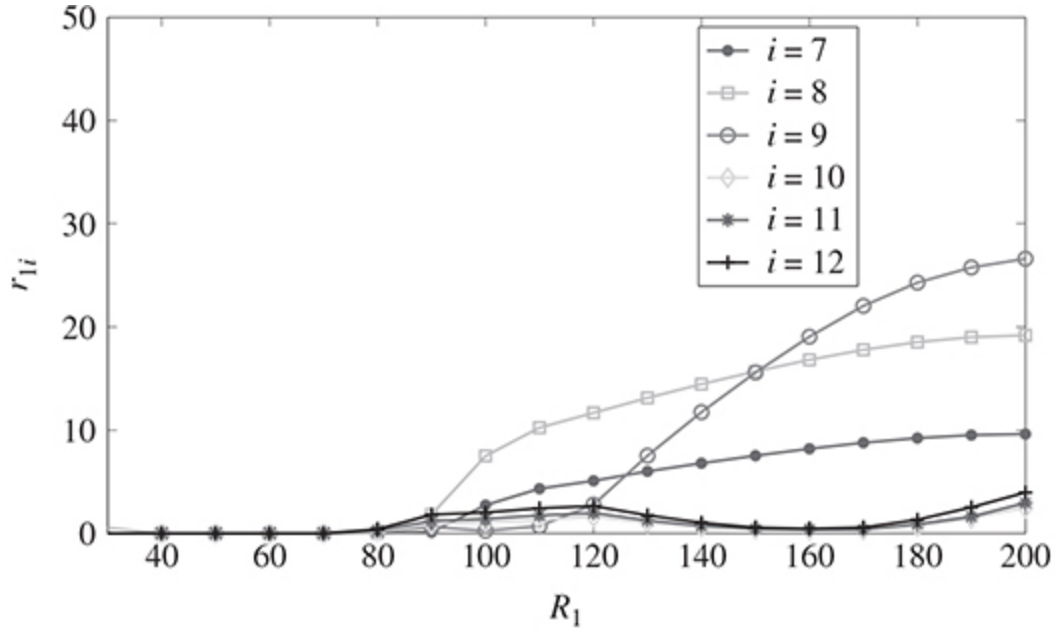
(a) The rates allocated r_{1i} from the 1st carrier eNodeB (i.e., the macro cell eNodeB) to users of the 1st group (i.e., $i = 1, 2, 3, 4, 5, 6$).



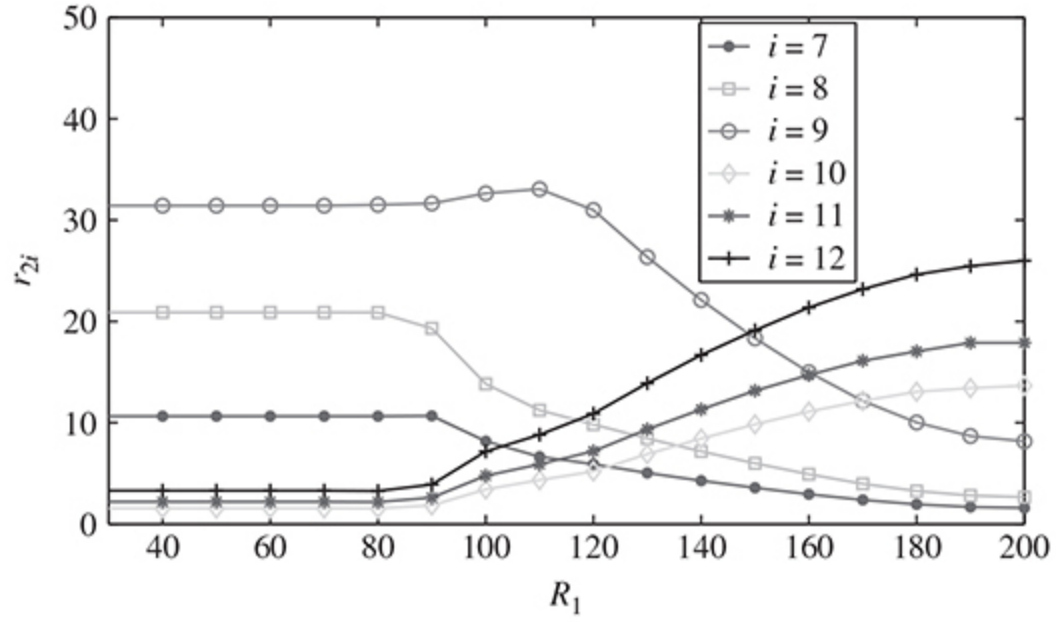
(b) The rates $r_{1i} + r_{2i}$ allocated from 1st and 2nd carriers eNodeBs (i.e., the macro cell and the small cell eNodeBs) to users of the 2nd group (i.e., $i = 7, 8, 9, 10, 11, 12$).

FIGURE 3.5 The allocated rates $\sum_{l=1}^{K} r_{li}$ in HetNetl of the two groups of users versus 1st carrier rate $30 < \boldsymbol{R_1} < 200$ with 2nd carrier rate fixed at $\boldsymbol{R_2} = 70$.

Figure 3.6 shows the rates allocated to the 2nd group users, located under the coverage area of both the macro cell and small cell eNodeBs, by each of the two carriers' eNodeBs with the increase in the 1st carrier eNodeB resources. In Figure 3.6(a) and 3.6(b), when the resources available at C2 eNodeB (i.e., R_2) is more than that at C1 eNodeB, we observe that most of the 2nd group rates are allocated by C2 eNodeB. However, the delay-tolerant applications are not allocated much resources since most of R_2 is allocated to the real-time applications. With the increase in C1 eNodeB resources R_1, we observe a gradual increase in the 2nd group rates allocated to real-time applications from C1 eNodeB and a gradual decrease from C2 eNodeB resources allocated to real-time applications. This shift in the RA increases the available resources in C2 eNodeB to be allocated to 2nd group delay tolerant applications by C2 eNodeB.



(a) The allocated rates r_{1i} from the 1st carrier eNodeB to the 2nd group of users.



(b) The allocated rates r_{2i} from the 2nd carrier eNodeB to the 2nd group of users.

FIGURE 3.6 The allocated rates in HetNet1 from C1 and C2 eNodeBs to the 2nd group of users with 1st carrier eNodeB rate $30 < \boldsymbol{R_1} < 200$ and 2nd carrier eNodeB rate fixed at R2 = 70.

Pricing Analysis and Comparison for 30 ≤ R_i ≤ 200 and R2 = 70

The following simulations are performed for HetNetl, we set ∞ = 10^{-3} and the 1st carrier eNodeB rate R_1 takes values between 30 and 200 with step of 10, and C2 eNodeB total rate is fixed at R_2 = 70. As discussed before, the users' allocated rates are proportional to the users' bids. Real-time application users bid higher than delay-tolerant application users due to their applications' nature and the utility proportional fairness policy. Therefore, the pricing which is proportional to the bids is traffic dependent, that is, when the demand by users increases, as a result the price increases and vice versa.

Figure 3.7 compares between the shadow price of C1 and C2 eNodeBs when using the proposed RA with joint CA approach with their shadow prices obtained when using the multistage RA with CA approach in [82-84]. For the RA with joint CA case, we observe that the shadow price of C1 eNodeB is higher than that of C2 eNodeB for R_1 < 80 and approximately equal for 80 ≤ R_1 ≤ 200, which shows how it is very efficient to use the joint CA approach for the pricing of the user. We also show how the prices decrease with the increase in the eNodeBs total rate. By using this traffic-dependent pricing, the network providers can flatten the traffic especially during peak hours by setting a traffic-dependent resource price, which gives an incentive for users to use the network during less-trafficked hours. On the other hand, for the multistage RA with CA approach, Figure 3.7 shows the changes in C1 and C2 eNodeBs shadow prices with R_1. When using the multistage RA with CA approach, all users are first allocated rates by the macro cell eNodeB, once C1 eNodeB is done allocating its resources C2 eNodeB starts allocating its resources only to the 2nd group users as they are located within its coverage area. Since the pricing method in multistage RA with CA approach is not optimal, this explains why the shadow prices of C1 and C2 eNodeBs, in Figure 3.7, when using the proposed RA with joint CA approach are less than their corresponding prices when using the multistage RA with CA approach. This shows how the proposed algorithm outperforms the algorithms presented in [82-84] as it guarantees that mobile users receive optimal price (minimum) for resources.

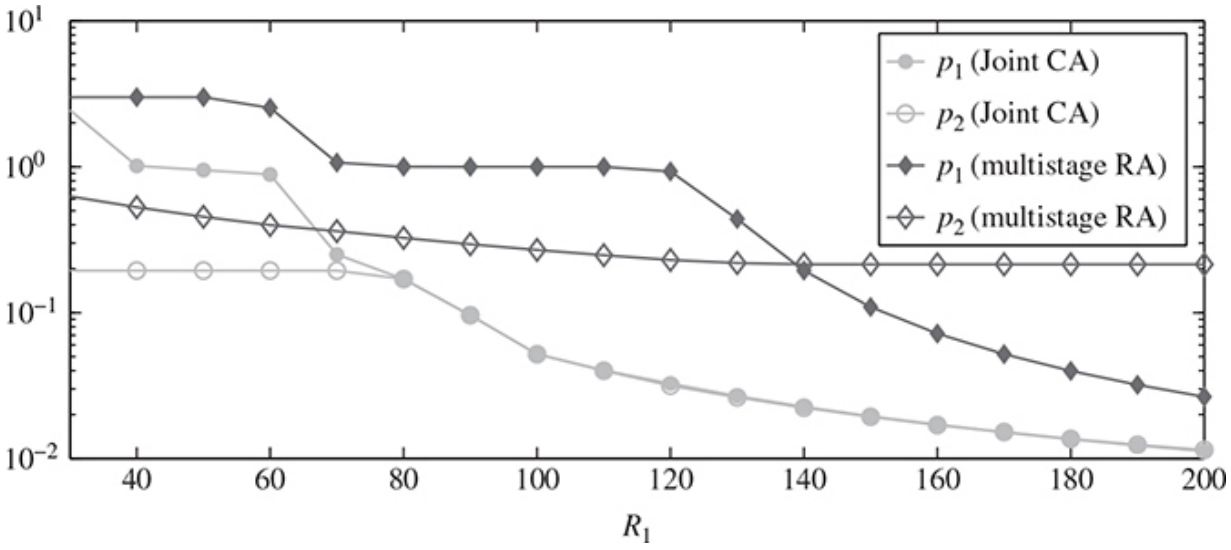


FIGURE 3.7 The 1st carrier shadow price p_1 and 2nd carrier shadow price p_2 in HetNet1 for both multistage RA with CA and joint RA methods with C1 eNodeB rate $30 < R1 < 200$ and C2 eNodeB rate $R2 = 70$.

3.7.2 Second Heterogeneous Network

The simulated cellular network in this section is a HetNet (HetNet2) that consists of two macro cells, two small cells, 20 active UEs, and four eNodeBs as shown in Figure 3.8. Macro cell 1 eNodeB has resources presented by carrier 1 (C1) with a maximum achievable rate $R1$, macro cell 2 eNodeB has resources presented by carrier 2 (C2) with a maximum achievable rate R_2, small cell 1 eNodeB has resources presented by C3 with a maximum achievable rate R_3, and small cell 2 eNodeB has the same resources as small cell 1 eNodeB presented by carrier 3 (C3) with a maximum achievable rate $R3$. Small cell 1 and small cell 2 do not intersect with each other, and therefore we consider frequency reuse where C3 resources can be used by the two eNodeBs to be allocated to UEs located in the small cells. In HetNet2, the UEs are divided into five groups. The 1st group of UEs (index $i = \{1,2,3,4\}$) is located in macro cell 1 under the coverage area of macro cell 1 eNodeB (C1), the 2nd group of UEs (index $i = \{9,10,11,12\}$) is located under the coverage of macro cell 2 eNodeB (C2), the 3rd group of UEs (index $i = \{5,6,7,8\}$) is located under the coverage of both macro cell 1 eNodeB (C1) and small cell 1 eNodeB (C3), the 4th group of UEs (index $i = \{13,14,15,16\}$) is located under the coverage of

both macro cell 2 eNodeB (C2) and small cell 2 eNodeB (C3), the 5th group of UEs (index i = {17,18,19,20}) is located under the coverage of both macro cell 1 eNodeB (C1) and macro cell 2 eNodeB (C2). Each UE is running either real-time or delay-tolerant applications represented by the utility functions shown in Figure 3.2. The utility function parameters used to represent the UEs applications for HetNet2 are summarized in Table 3.2.

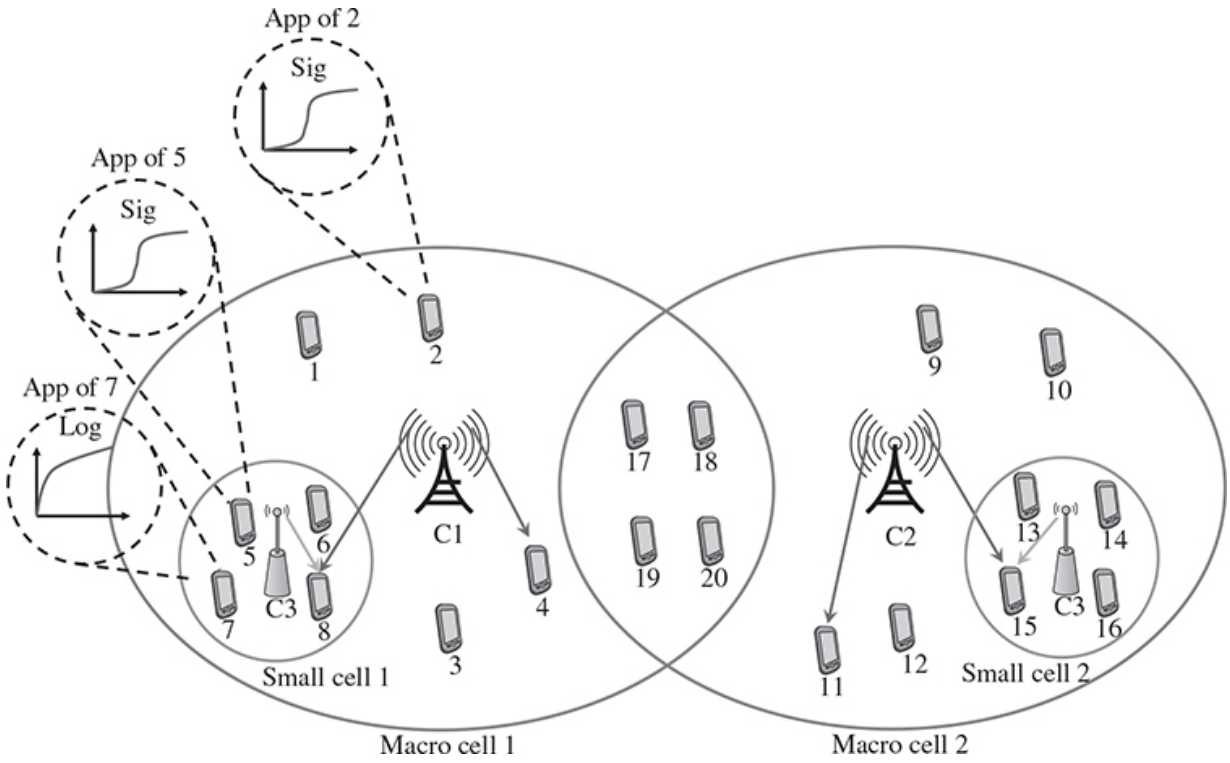


FIGURE 3.8 System model for HetNet2 with five groups of users. The 1st group with UE indexes i = {1, 2, 3, 4}, 2nd group with UE indexes i = {9, 10, 11, 12}, 3rd group with UE indexes i = {5, 6, 7, 8}, 4th group with UE indexes i = {13, 14, 15, 16}, and 5th group with UE indexes i = {17, 18, 19, 20}.

In the following simulations, we set $\infty = 10^{-3}$, the 1st carrier eNodeB rate R_1 takes values between 30 and 200 with step of 10, the 2nd carrier eNodeB rate is fixed at $R_2 = 150$, the 3rd carrier rate (i.e., for small cell 1 and small cell 2 eNodeBs) is fixed at $R_3 = 55$. Figures 3.9 to 3.13 show the final allocated optimal rates $r_i = \sum_{l=1}^{K} r_{li}$ of different users with different 1st carrier eNodeB total rate R_1 and observe how the behavior of simulation

matches our derived mathematical results. Figure 3.9 shows the rates allocated to the 1st group of UEs by only C1 eNodeB since other carriers are not within these users' range, we observe the increase in the rate allocated to these users with the increase in R_1. Figure 3.10 shows the final allocated rates to the 3rd group of UEs by both C1 and C2 eNodeBs. Since these users located under the coverage area of both the macro cell and the small cell, they are allocated rates jointly using the proposed RA with joint CA approach. Figure 3.11 shows the rates allocated to the 2nd group of UEs by only C2 eNodeB since other carriers are not within these users' range, we observe the increase in the rate allocated to these users with the increase in R_1. Figure 3.12 shows the final allocated rates to the 4th group of UEs by both C2 of macro cell 2 eNodeB and C3 of small cell 2 eNodeB. Since these users are located under the coverage of both macro cell 2 and small cell 2, they are allocated rates jointly using the proposed RA with joint CA approach. Figure 3.13 shows the final allocated rates to the 5th group of UEs by both C1 and C2 eNodeBs. We also observe from Figures 3.9 to 3.13 that by using the RA with joint CA algorithm, no user is allocated zero rate. We also observe that by using the utility proportional fairness policy, the majority of the eNodeBs' resources are allocated to the UEs with real-time applications until they reach their inflection rates. The eNodeBs then allocate more resources to the UEs with delay-tolerant applications [253].

Applications Utilities Parameters for UEs in HetNet2		Users Indexes
Sig2	Sig $a = 3,\ b = 20$	$i = \{1, 5, 9, 13, 17\}$
Sig3	Sig $a = 1,\ b = 30$	$i = \{2, 6, 10, 14, 18\}$
Log2	Log $k = 3,\ r_{max} = 100$	$i = \{3, 7, 11, 15, 19\}$
Log3	Log $k = 0.5,\ r_{max} = 100$	$i = \{4, 8, 12, 16, 20\}$

TABLE 3.2 Users and Their Applications Utilities in HetNet2

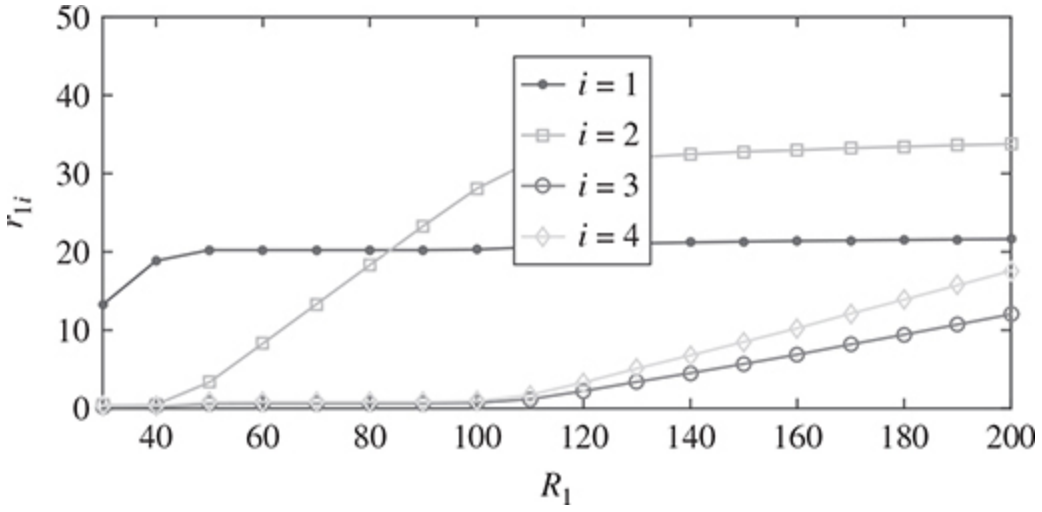


FIGURE 3.9 The rates allocated r_{1i} from the 1st carrier eNodeB (i.e., macro cell 1 eNodeB) to users of the 1st group (i.e., i = 1, 2,3,4). HetNet2 allocated rates $\sum_{l=1}^{K} r_{li}$ of the five groups of users versus 1st carrier rate 30 < R_1 < 200 with 2nd carrier rate fixed at R_2 = 150 and 3rd carrier rate fixed at R_3 = 55.

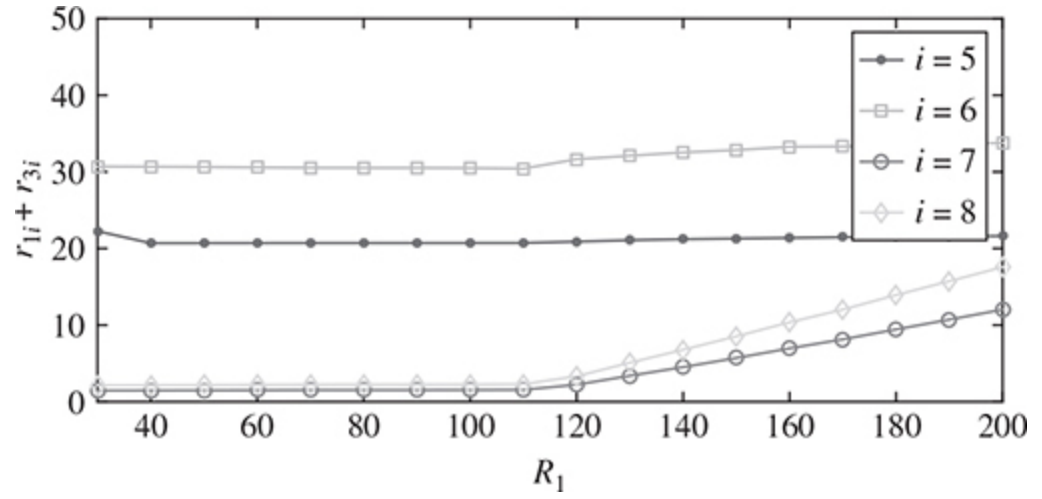


FIGURE 3.10 The rates $r_{1i} + r_{3i}$ allocated from 1st and 3rd carriers eNodeBs (i.e., macro cell 1 and small cell 1 eNodeB) to users of the 3rd group (i.e., i = 5, 6, 7, 8).

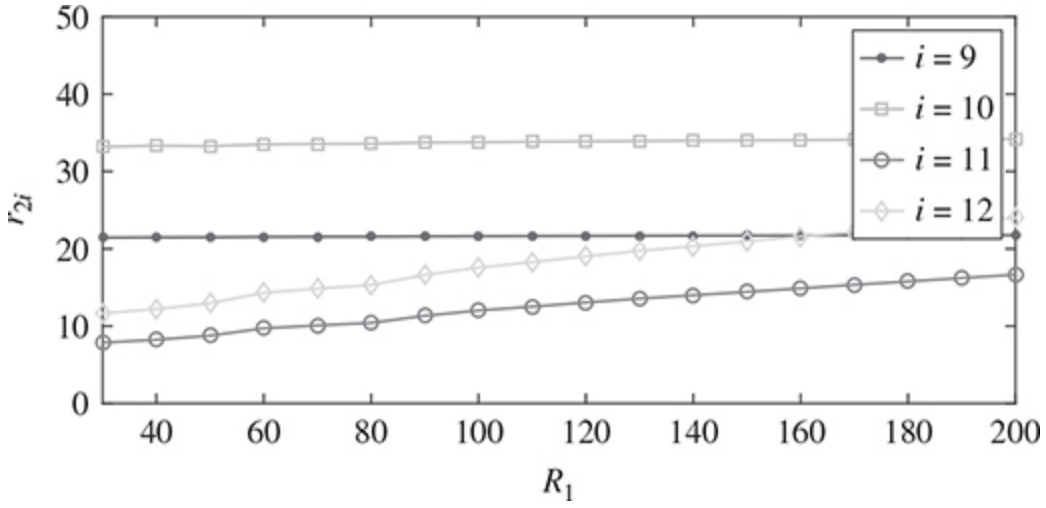


FIGURE 3.11 The rates allocated r_{2i} from the 2nd carrier eNodeB (i.e., macro cell 2 eNodeB) to users of the 2nd group (i.e., ***i*** = 9,10,11,12).

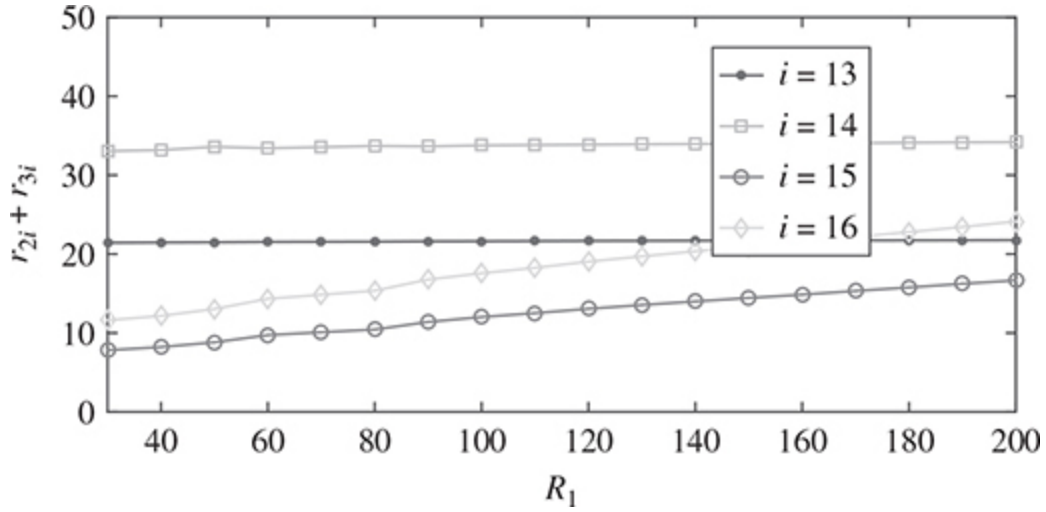


FIGURE 3.12 The rates $r_{2i} + r_{3i}$ allocated from 2nd and 3rd carriers eNodeBs (i.e., macro cell 1 and small cell 2 eNodeBs) to users of the 4th group (i.e., i = 13, 14, 15, 16).

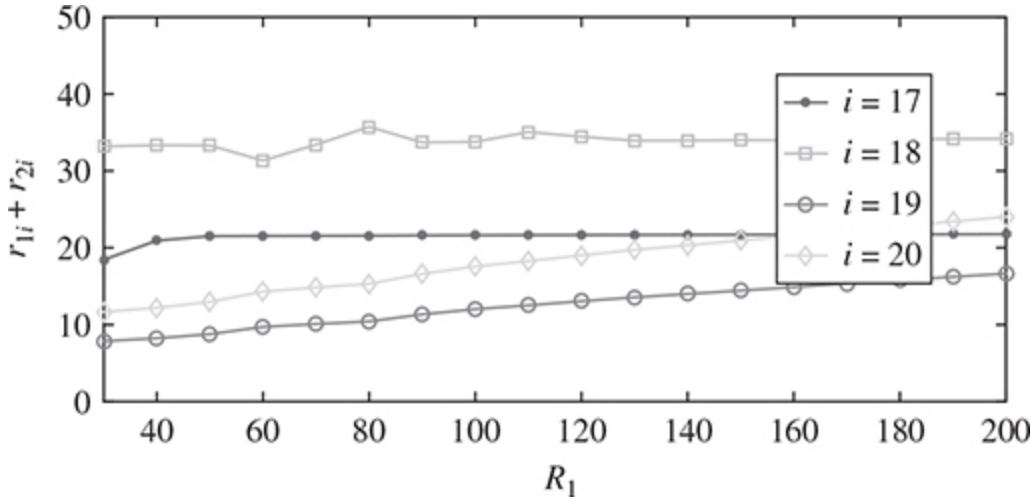


FIGURE 3.13 The rates r_{2i} **+** $\boldsymbol{r_{4i}}$ allocated from 1st and 2nd carriers eNodeBs (i.e., macro cell 1 and macro cell 2 eNodeBs) to users of the 5th group (i.e., $\boldsymbol{i}$ = 17,18,19, 20).

3.8 Conclusion

In this chapter, we introduced a novel RA optimization problem with joint CA in cellular networks. We considered mobile users running real-time and delay-tolerant applications with utility proportional fairness allocation policy. We proved that the global optimal solution exists and is tractable for mobile stations with logarithmic and sigmoidal-like utility functions. We presented a novel robust distributed algorithm for allocating resources from different carriers optimally among the mobile users. Our algorithm ensures fairness in the utility percentage achieved by the allocated resources for all users. Therefore, the algorithm gives priority to users with adaptive real-time applications while providing a minimum QoS for all users. In addition, the proposed RA with joint CA algorithm guarantees allocating resources from different carriers with the lowest resource price for the user. We analyzed the convergence of the algorithm with different network trafic densities and presented a robust algorithm that overcomes the fluctuation in allocation during peak traffic hours. We showed through simulations that our algorithm converges to the optimal RA and that the proposed algorithm outperforms the multistage RA with CA algorithms presented in [82-84] as it guarantees that mobile users receive optimal price for the allocated resources.

[1]The content in this chapter is reproduced with permission after modifications (license number 4762090250918). For the original article, refer to [227].

CHAPTER 4

Optimal Bidding Strategy for Secure Spectrum Auctions[1]

Haya Shajaiah, Ahmed Abdelhadi, and Charles Clancy

In this chapter, we propose an optimal bidding mechanism for a truthful secure spectrum auction in which bidders are base stations (BSs) that seek to obtain additional temporary resources by participating in the spectrum auction. By using the proposed bidding strategy, each bidder first determines its true bidding price for each number of spectrum bands it is bidding for and submits its corresponding encrypted bidding value. The proposed bidding mechanism takes into consideration that BSs participating in the spectrum auction have permanent resources and will be aggregating their winning spectrum bands (temporary resources) with the permanent resources, based on a non-adjacent carrier-aggregation scenario when allocating optimal rates to active users under their coverage area. We consider a secure spectrum auction that uses homomorphic encryption through Pailliar cryptosystem to prevent possible fraud and bid-rigging. We also focus on providing an efficient resource management solution to distribute the auctioned resources among end users [i.e., users equipment (UEs)] in order to improve the UEs' quality of experience (QoE). Furthermore, a resource allocation based on carrier-aggregation approach is proposed to allocate the BS's permanent spectrum resources as well as its temporary resources (i.e., the auctioned underutilized-frequency bands) optimally among mobile users.

4.1 Introduction

Previous research effort has considered designing secure spectrum auctions. In [123-125], homomorphic encryption is used to provide security in traditional auctions. The authors in [126] proposed a secure spectrum auction design **THEMIS** that leverages Paillier cryptosystem to avoid possible frauds and bid-rigging. Later in [198], a secure spectrum auction framework **MTSSA** is proposed for multitier spectrum sharing systems. **MTSSA** allows spectrum reusability among multiple service providers and provides a truthful secure spectrum auction by assuming that each bidder submits its true bidding value. However, **MTSSA** does not provide a bidding strategy for BSs participating in the spectrum auction. Given that truthfulness is a dominant property in a secure spectrum auction, as it prevents insincere bidders from manipulating the auction, it is important to design a bidding mechanism to be used by bidders to determine their true bidding values.

In this chapter, we focus on providing an optimal bidding strategy for BSs participating in a truthful secure spectrum auction. BSs that belong to different wireless system providers (WSPs) and are interested in additional resources participate in the spectrum auction. The auctioneer auctions the spectrum bands to BSs that belong to different WSPs. We use a spectrum auction mechanism that allows spectrum reuse among multiple WSPs and optimizes the usage of spectrum resources by managing intra-WSP and inter-WSP interference. The auctioneer carries out a secure spectrum auction for its available underutilized spectrum bands. Based on the auction's result, the auctioneer allocates each of the winning bidders the corresponding spectrum bands and charges them for the allocated resources. The proposed bidding strategy is essential in a truthful secure spectrum auction as it guarantees that bidders submit their true bidding values preventing insincere bidders from manipulating the auction. By using the proposed bidding strategy, each BS participating in the spectrum auction calculates its true bidding value for the number of spectrum bands it is bidding for based on its demand for these resources. The BS's decision regarding its demand is driven by the traffic of the active UEs, located under its coverage area, that are subscribing for mobile services from that BS. In addition, we provide an efficient resource management solution to enable BSs participating in the spectrum auction to distribute their temporary auctioned resources as well as their permanent resources optimally among UEs based on a carrier-aggregation scenario [255-258].

Our contributions in this chapter are summarized as:

- We propose an optimal bidding mechanism for determining true bidding values to be used in secure spectrum auctions by BSs, which belong to different WSPs, participating in a spectrum auction seeking additional resources to improve the quality of experience (QoE) for active UEs located under their coverage area [259-262]. The BS's true bidding values are determined based on the number of spectrum bands it is bidding for, the applications traffic of users under its coverage area, and the quantity of bidder's permanent resources.
- We show that the proposed bidding mechanism is a demand-based one where the bidding price per spectrum band is related to the BS's demand for additional resources. We prove that by using the proposed bidding mechanism, when a BS bids for certain number of spectrum bands n, its bidding price of the *Ith* spectrum band (/ *e* {1,2,.., *n* — 1}) is greater than its bidding price of the (/ + 1)th spectrum band as the BS's price per spectrum band depends on its demand for that spectrum band.
- We present a resource allocation based on carrier-aggregation approach to determine the BS's optimal aggregated rate allocated to each UE from both the BS's permanent resources and the BS's winning auctioned spectrum resources.
- We show through simulation results the performance of the proposed optimal bidding strategy when used by BSs participating in a secure spectrum auction and show that the spectrum auction achieves an efficient spectrum utilization, revenue, and bidders' satisfaction.

4.2 System Model

We consider a spectrum sharing scenario where a federal agency leases its underutilized spectrum bands on a long-term basis to a broker, which plays the role of an auctioneer and auctions the spectrum bands to BSs that belong to different WSPs and located in the same geographical area. Let *L* denote the number of WSPs with coverage areas within the auction's geographical region. Each WSP provides wireless services to multiple cellular cells through BSs where one BS is located in the middle of each cellular cell. Each BS has permanent resources assigned to it by its WSP

and each BS allocates its resources to UEs that belong to its WSP and located within its coverage area. Each BS with a high-traffic volume (i.e., during peak hours) and scarce permanent resources can participate in the spectrum auction by submitting its bidding price to the auctioneer. Let $\mathcal{K}$ denote the set of BSs, which belong to WSP *l*, participating in the spectrum auction and let $\mathcal{K} = \mathcal{K}^1 \bigcup \mathcal{K}^2 \bigcup ... \bigcup \mathcal{K}^L$ denote the set of the *L* WSPs' BSs participating in the spectrum auction where $K = |\mathcal{K}|$ denotes the number of BSs in $\mathcal{K}$. Furthermore, let $\mathcal{M}_k$ be the set of UEs subscribing for mobile services from the *k*th BS in $\mathcal{K}$. The set of auctioneer's spectrum bands is given by $\mathcal{N}$, where $N = |\mathcal{N}|$ denotes the number of the auctioneer's available spectrum bands. Let R_k^p denote the total achievable rate of the permanent resources of BS *k* at the time during which the auction takes place.

In this chapter, we consider a multiband spectrum auction, similar to the one presented in [198], where each BS can bid for a single or multiple spectrum bands in the set $\mathcal{N}$ auctioned by the broker (auctioneer). Once the auction takes place, each BS in $\mathcal{K}$ submits its bids to the auctioneer. Let $\alpha = \{\alpha_1, \alpha_2, ...\}$ be the allocation set for the *N* spectrum bands, where $\alpha_j \in \alpha$ is an allocation in α that is given by $\alpha_j = (\alpha_j(1), ..., \alpha_j(k), ..., \alpha_j(K))$ and $\alpha_j(k)$ represents the number of spectrum bands that the *k*th BS in $\mathcal{K}$ is bidding for. For example, for $\mathcal{K} = \{1,2,3\}$ and $\mathcal{N} = \{a, b\}$ we have $\alpha = \{\alpha_1 = (2,0,0), \alpha_2 = (0,2,0), \alpha3 = (0,0,2), \alpha4 = (1,1,0), \alpha5 = (1,0,1), \alpha6 = (0,1,1)\}$. Each BS $k \in \mathcal{K}$ creates its bidding vector $\mathbf{b_k} = [b_k(\alpha_1), b_k(\alpha_2), ...]$ and submits an encrypted bidding vector $\hat{\mathbf{b}}_k = [\hat{b}_k(\alpha_1), \hat{b}_k(\alpha_2), \ldots]$ for the allocations in **α,** where $\hat{b}_k(\alpha_j)$ is the encrypted bidding value for the actual bid $b_k(\alpha_j)$. In the above example, $\mathbf{b_1} = [6,0,0,3,3,0]$ indicates that BS 1 bids 6 for allocation a_1, 0 for allocation α_2, 0 for allocation α_3, 3 for allocation α_4, 3 for allocation a_5, and 0 for allocation α_6. We assume that the BSs treat different spectrum bands similarly. Let $ek(\alpha_j)$ represent the *k*th BS true evaluation value for allocation αj and let p_k denote the actual price that the *k*th BS in $\mathcal{K}$ pays to the auctioneer. The *k*th BS utility is given by $u_k = e_k(\alpha_j) - p_k$, which is the difference between the *k*th BS true evaluation value and the actual price the BS pays to the auctioneer for the allocated spectrum

bands for allocation α_j . The auctioneer's revenue is given by $Rev = \sum_{k=1}^{K} p_k$ which is the sum of all BSs' payments from the spectrum sale. Table 4.1 summarizes some of the notations used in the design.

$\mathcal{N}$	Frequency bands set
$\mathcal{K}^l$	Set of all BSs that belong to WSP l
$\mathcal{K}$	Set of all BSs that belong to the L WSPs, $\mathcal{K} = \mathcal{K}^1 \cup \mathcal{K}^2 \cup \ldots \cup \mathcal{K}^L$
$\mathcal{M}_k$	Set of UEs subscribing for mobile services from the kth BS in $\mathcal{K}$
R_k^p	Total achievable rate of the permanent resources of BS k
$\boldsymbol{\alpha}$	Allocation set $\boldsymbol{\alpha} = \{\alpha^1, \alpha^2, \ldots\}$
$\mathbf{b}_k$	BS k bidding vector for the allocation set $\boldsymbol{\alpha}$
$\hat{\mathbf{b}}_k$	BS k encrypted bidding vector for the allocation set $\boldsymbol{\alpha}$
$\hat{b}_k(\alpha_j)$	BS k encrypted bidding value for the actual bid $b_k(\alpha_j)$
$e_k(\alpha_j)$	True evaluation value of BS k for allocation α_j
p_k	Price charged by the auctioneer to BS k
u_k	BS k utility, $u_k = e_k(\alpha_j) - p_k$
Rev	Auctioneer's revenue, $Rev = \sum_{k=1}^{K} p_k$

TABLE 4.1 Key Symbols in This Chapter

Once the auctioneer shares with all WSPs' BSs (i.e., BSs located within the auction geographical region) the number of its spectrum bands N, each BS decides whether to participate in the spectrum auction or not based on the current traffic of the UEs located under its coverage area (i.e., UEs in $\mathcal{M}_k$) and its current permanent available resources R_k^p. If the BS's R_k^p value is considered scarce for the current active UEs' demand of resources, the BS decides to participate in the spectrum auction and submit its bidding values for all possible allocations in $\boldsymbol{\alpha}$. We assume that the kth BS's decision on whether to participate in the spectrum auction or not is driven by its system utility; that is, if the total system QoE when the UEs in $\mathcal{M}_k$ are allocated resources only from the BS's permanent resources is below a minimum expected predefined value, then the BS decides to participate in

the spectrum auction in order to obtain additional resources and allocates both of its permanent resources as well as its auctioned resources to the UEs in $\mathcal{M}_k$ based on a carrier-aggregation scenario. As in [198], all bidders submit their bidding values to the auctioneer through an intermediate secure gateway. In order to consider the spectrum reusability property [32, 43], the secure gateway builds an interference conflict graph, which consists of nodes that represent all BSs participating in the auction. Each BS (node) in the interference conflict graph is connected with other nodes located within its coverage area, which indicates that the auctioneer cannot allocate the *k*th BS spectrum bands similar to the ones simultaneously allocated to any other BS connected to BS *k* in the interference conflict graph. The interference conflict graph can be constructed using a physical or a protocol channel model [221]. Figure 4.1 shows two WSPs located within the auction's geographical region with all of their BSs participating in the auction. An interference conflict graph for the two WSPs' BSs is shown in the same figure with an illustration of one subnet. The auctioneer runs the spectrum auction in one subnet after another, where a subnet consists of one root BS (i.e., BS1 in Figure 4.1) and all other nodes connected to it in the interference conflict graph that are not previously considered root BSs.

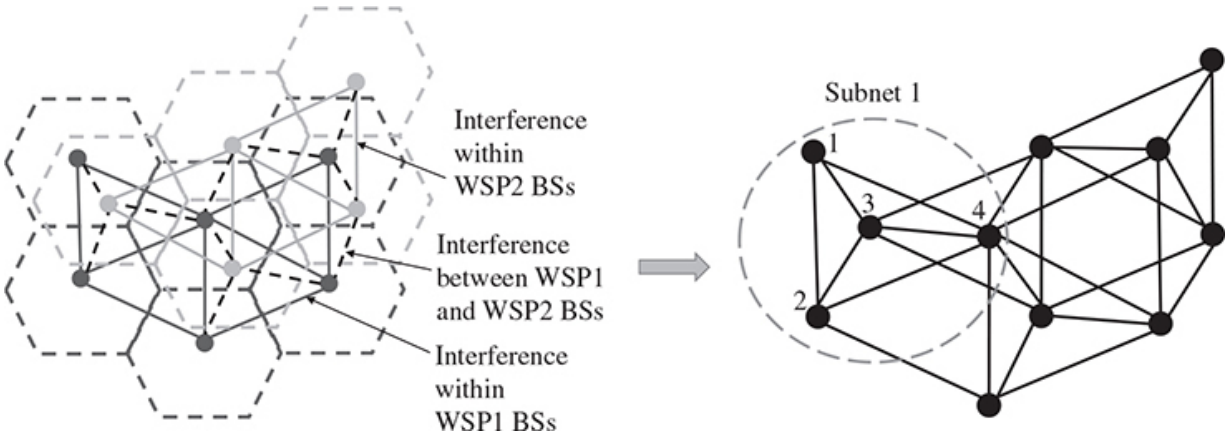


FIGURE 4.1 Frequency conflict graph for two WSPs's BSs participating in the spectrum auction, where nodes represent BSs and edges represent mutual interference between end points (BSs) with an illustration of one subnet; that is, subnet 1 which consists of BSs 1, 2, 3, and 4, where BS 1 is the root BS.

4.3 Spectrum Sharing through Secure and Truthful Spectrum Auction

In this section, we present a spectrum sharing system that provides an efficient sharing of spectrum resources with commercial WSPs using a secure truthful spectrum auction. Figure 4.2 shows the proposed spectrum sharing model that is performed in the following steps: (1) Each BS that belongs to a WSP within the auction region and decides to participate in the spectrum auction, determines its optimal true bidding values (by using the proposed optimal bidding mechanism), and submits them to the auctioneer through the secure gateway. (2) The auctioneer runs a secure spectrum auction **MTSSA** [198] in one subnet after another. (3) Each BS is allocated the spectrum bands it won and charged for the allocated resources. (4) Each BS allocates its winning auctioned spectrum bands (temporary resources) along with its permanent resources to the UEs under its coverage area based on a carrier-aggregation scenario and charges the UEs for the allocated resources.

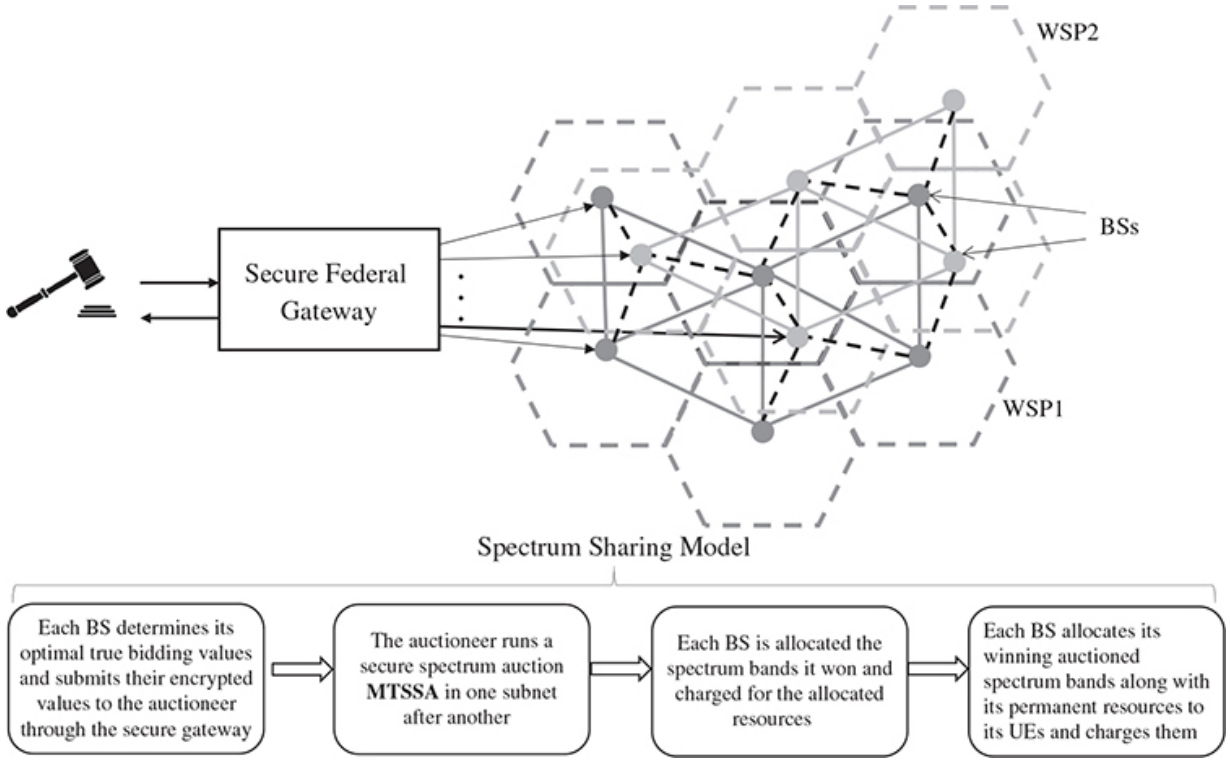

WSP2
BSs
WSP1
Secure Federal Gateway
Spectrum Sharing Model
Each BS determines its optimal true bidding values and submits their encrypted values to the auctioneer through the secure gateway
The auctioneer runs a secure spectrum auction MTSSA in one subnet after another
Each BS is allocated the spectrum bands it won and charged for the allocated resources
Each BS allocates its winning auctioned spectrum bands along with its permanent resources to its UEs and charges them

FIGURE 4.2 Spectrum sharing model through a truthful and secure spectrum auction with BSs that belong to two WSPs participating in the auction.

The optimized resource allocation process for the aforementioned spectrum sharing system is performed by a collaboration between the bidding BSs and the auctioneer in two stages. One is performed in a distributed manner and the other is performed in a centralized manner. Each bidding BS optimizes its own utility function, which is a distributed manner whereas the BSs' bidding and spectrum allocation are conducted at the auctioneer, which is centralized. The details of this resource allocation process as well as the optimal bidding procedure are discussed in the next section.

4.3.1 An Optimal Mechanism for Determining True Bidding Values

Each BS decides whether its primary resources are sufficient or not based on its available permanent resources and the traffic of the applications running on the UEs subscribing for mobile services from that BS. Each BS in $\mathcal{K}$ located within the auction region informs the auctioneer about its interest in participating in the spectrum auction seeking additional resources. Once the auctioneer runs the spectrum auction, each of the BSs participating in the auction receives the number of the auctioneer's spectrum bands N as well as the number of all bidders K participating in the auction.

Each BS $k \in \mathcal{K}$ performs a resource allocation process using Utility Proportional Fairness (UPF) approach to determine its assigned resources from its permanent resources to each active UE $i \in \mathcal{K}_k$. Utility functions are used to express the user's satisfaction with its allocated rate [135,159,241,244]. Let $U_i(r_i)$ represents the ith user application utility function of its allocated rate r_i, where sigmoidal-like utility functions are used to represent real-time applications and logarithmic utility functions are used to represent delay-tolerant applications. These utility functions have the following properties: (1) $U_i(0) = 0$ and $U_i(r_i)$ is an increasing function of r_i. (2) $U_i(r_i)$ is twice continuously differentiable in ri and bounded above. We use normalized sigmoidal-like utility functions, as in [82, 158], that are expressed as

$$U_i(r_i) = c_i \left(\frac{1}{1 + e^{-a_i(r_i - b_i)}} - d_i \right) \tag{4.1}$$

where $c_i = \frac{1+e^{a_i b_i}}{e^{a_i b_i}}$ and $d_i = \frac{1}{1+e^{a_i b_i}}$, so it satisfies $U_i(0) = 0$ and $U_i(\infty) = 1$. a_i, b_i, and d_i are the sigmoidal-like utility parameters that vary based on the type and rate requirement of the real time application that the sigmoidal function is representing. The normalized sigmoidal-like function has an inflection point at $r_i^{\inf} = b_i$. In addition, we use the normalized logarithmic utility functions, used in [82,158], that are expressed as

$$U_i(r_i) = \frac{\log(1 + \beta_i r_i)}{\log\left(1 + \beta_i r_i^{\max}\right)} \tag{4.2}$$

where r_i^{max} gives 100% utilization and β_i is the rate of increase of utility percentage with allocated rates that varies based on the user application. So, it satisfies
$Ui(0) = 0$ and $Ui(r_i^{ma}) = 1$.

We use a UPF resource allocation optimization problem to find the kth BS assigned resources to each of the UEs in M_k and the BS's price per unit bandwidth. The UPF resource allocation optimization problem that is used for assigning the kth BS permanent resources is given by

$$\begin{aligned} \max_{\mathbf{r}_k^p} \quad & \prod_{i=1}^{|\mathcal{M}_k|} U_i\left(r_{i,k}^p\right) \\ \text{subject to} \quad & \sum_{i=1}^{|\mathcal{M}_k|} r_{i,k}^p \le R_k^p \\ & 0 \le r_{i,k}^p \le R_k^p, \quad i = 1, 2, \ldots, |\mathcal{M}_k| \end{aligned} \tag{4.3}$$

where $\mathbf{r}_k^p = \{r_{1,k}^p, r_{2,k}^p, \ldots, r_{|\mathcal{M}_k|,k}^p\}$, $r_{i,k}^p$ is the achievable rate of the ith UE in M_k from BS k assignment to that UE from its permanent resources, $|\mathcal{M}.k|$ is the number of active UEs under the coverage area of BS k and $R^P{}_K$ is the maximum achievable rate of the kth BS from its

available permanent resources; that is, $R^P{}_K$ is the sum of all rates achieved by all users from allocating the *k*th BS available permanent resources. It is assumed that $R^p{}_K$ is known by BS *k* and that $R^p{}_K$ does not change its value during the auction allocation process. The objective function of the above UPF resource allocation is to maximize the entire cell utility when allocating the BS's resources and achieve UPF such that none of the UEs is allocated zero resources. Therefore, it guarantees a minimum QoS for each UE. Real time applications are given priority when allocating the BS's resources due to the nature of their utility functions used to represent their applications. The objective function in optimization problem (4.3) is equivalent to $r_i^{\inf} = b_i$. Optimization problem (4.3) is a convex optimization problem and there exists a unique tractable global optimal solution as shown in [82,158]. From optimization problem (4.3), we have the Lagrangian as follows:

$$L_p(\mathbf{r}_k^p, p_k^p) = \sum_{i=1}^{|\mathcal{M}_k|} \log U_i(r_{i,k}^p) - p_k^p \left(\sum_{i=1}^{|\mathcal{M}_k|} r_{i,k}^p + z_k^p - R_k^p \right) \tag{4.4}$$

where $z_k^p \geq 0$ is the slack variable and $p^p{}_k$ is the Lagrange multiplier, which represents the shadow price (price per unit bandwidth) of BS *k* for its assigned resources from its permanent available resources. The solution of optimization problem (4.3) is given by the values $r^p{}_{ik}$, which are the solution of $\frac{\partial \log U_i(r_{i,k}^p)}{\partial r_{i,k}^p} = p_k^p$ and are the intersection of the time varying shadow price, horizontal line $y = p_k^p$, with $y = \frac{\partial \log U_i(r_{i,k}^p)}{\partial r_{i,k}^p}$ geometrically. Once BS *k* performs the UPF resource assignments for its permanent resources, each UE in $\mathcal{M}_k$ will be assigned $r_{i,k}^{p,\text{opt}} = r_{i,k}^p$ rate but not yet allocated its assigned resources. As mentioned above, we

assume that each BS $k \in \mathcal{K}$ is demanding additional resources, and therefore will be participating in the spectrum auction; that is, the *k*th BS's cell utility obtained from the assigned resources $r_{i,k}^{p,\mathrm{opt}}$ is less than the minimum required utility.

Each BS uses the information it receives from the auctioneer regarding the number of all bidders *K* and the number of the auctioneer's spectrum bands *N* and uses them to create the allocation set **α.** For the number of spectrum bands $n = \alpha_j(k)$ (i.e., $n \leq N$) that corresponds to BS *k* in the allocation α_j, BS *k* determines the maximum achievable rate $R_{k,n'}^{t}$, if BS *k* allocates these temporary resources (i.e., auctioned resources) to its UEs. We assume that each BS *k* calculates its bidding price for certain allocation *aj* based on the number of spectrum bands that corresponds to that BS (i.e., *αj(k))* regardless of the number of spectrum bands that correspond to other BSs in the same allocation α_j. Therefore, BS *k* bidding price will be the same for all allocations $\alpha_j \in \alpha$ that have similar $\alpha_j(k)$ values. In order for BS *k* to determine its true bidding price that needs to be submitted to the auctioneer, it uses a UPF resource allocation with carrier aggregation to find its aggregated assigned resources from both its permanent resources R_k^p and its auctioned resources $R_{k,n'}^{t}$, assuming that this BS will be winning its corresponding number of spectrum bands in that allocation (i.e., $\alpha_j(k)$). Additionally, each BS also determines the price per unit bandwidth for the temporary auctioned resources based on resource allocation with carrier-aggregation optimization and calculates its bidding value for each allocation that has $\alpha_j(k) = n$ based on that price. The *k*th BS's UPF resource allocation optimization problem that is used for assigning the temporary auctioned resources $R^p{}_{k\,n}$ that corresponds to *n* spectrum bands (n ≤ N) is given by:

$$\max_{\mathbf{r}_{k,n}^t} \quad \prod_{i=1}^{|\mathcal{M}_k|} U_i\left(r_{i,k,n}^t + r_{i,k}^{p,\text{opt}}\right)$$
$$\text{subject to} \quad \sum_{i=1}^{|\mathcal{M}_k|} r_{i,k,n}^t \le R_{k,n}^t \tag{4.5}$$
$$0 \le r_{i,k,n}^t \le R_{k,n}^t, \quad i = 1, 2, \ldots, |\mathcal{M}_k|$$

where $\mathbf{r}_{k,n}^t = \{r_{1,k,n}^t, r_{2,k,n}^t, \ldots, r_{|\mathcal{M}_k|,k,n}^t\}$, $r_{i,k,n}^t$ is the achievable rate of the ith UE in $\mathcal{K}k$ from BS k assignment to that UE from its temporary auctioned resources, $|\mathcal{K}k|$ is the number of UEs that will be assigned temporary auctioned resources by BS k and $R^t_{k,n}$ is the maximum achievable rate of the kth BS from the auction resources. The objective function of the above optimization problem is to maximize the entire cell utility when allocating the BS's temporary resources. The RA optimization problem (4.5) is based on carrier aggregation. It seeks to maximize the multiplication of the utilities of the rates allocated to UEs in M_k by BS's permanent and auctioned resources. UPF is used to guarantee that none of the UEs will be allocated zero resources and real-time applications are given priority when allocating the BS's auctioned resources. The objective function in optimization problem (4.5) is equivalent to $\max_{\mathbf{r}_{k,n}^t} \sum_{i=1}^{|\mathcal{M}_k|} \log U_i(r_{i,k,n}^t + r_{i,k}^{p,\text{opt}})$. Optimization problem (4.5) is a convex optimization problem and there exists a unique tractable global optimal solution [82,158, 263-265]. From optimization problem (4.5), we have the Lagrangian as follows:

$$L_t(\mathbf{r}_{k,n}^t, p_{k,n}^t) = \sum_{i=1}^{|\mathcal{M}_k|} \log U_i(r_{i,k,n}^t + r_{i,k}^{p,\text{opt}}) - p_{k,n}^t \left(\sum_{i=1}^{|\mathcal{M}_k|} r_{i,k,n}^t + z_{k,n}^t - R_{k,n}^t \right) \quad (4.6)$$

where $z_{k,n}^t \geq 0$ is the slack variable and $p^t_{k,n}$ is the Lagrange multiplier, which represents the price per unit bandwidth of BS k for its assigned resources from its temporary resources $R^t_{k,n}$. The solution of optimization problem (4.5) is given by the values $r^t_{i,k,n}$ that solve equation $\frac{\partial \log U_i(r_{i,k,n}^t + r_{i,k}^{p,\text{opt}})}{\partial r_{i,k,n}^t} = p_{k,n}^t$ and are the intersection of the time varying shadow price, horizontal line $y = p^t_{k,n}$, with the curve $y = \frac{\partial \log U_i(r_{i,k,n}^t + r_{i,k}^{p,\text{opt}})}{\partial r_{i,k,n}^t}$ geometrically.

Once BS k is done performing the resource assignment with carrier-aggregation process for each possible number of auctioned spectrum bands n based on optimization problem (4.5), BS k calculates each bidding value $b_k(aj)$ as the following:

$$b_k(\alpha_j) = \sum_{l=1}^{n} D * p_{k,l}^t \quad \text{where} \quad n = \alpha_j(k) \quad (4.7)$$

where D is the number of unit bandwidths in one spectrum band and $p^t_{k,l}$ is the price per unit bandwidth of the lth spectrum band; $l = \{1,2,..., n\}$. After calculating all bidding values $b_k(\alpha_j)$, BS k creates a bidding vector $\mathbf{b_k} = [b_k(\alpha_1), b_k(\alpha_2),...]$ for the allocations in $\boldsymbol{\alpha}$ and submits its corresponding encrypted bidding vector $\hat{\mathbf{b}}_k$ to the secure gateway. Algorithm 4 summarizes the kth BS procedure for determining its optimal bidding values for the allocations in $\boldsymbol{\alpha}$. Algorithm 4 is executed by each bidder (BS)

and its computational complexity is directly related to the number of auctioneer's spectrum bands *N* as each BS will be computing a bidding price for each number of spectrum bands $n \leq N$; that is, *N* different values of bidding prices.

Once the secure gateway receives the encrypted bidding values from all bidders, it starts performing spectrum bands allocation as will be discussed in Section 4.3.2. The auctioneer then decides the winning BSs, allocates them the corresponding spectrum bands, and charges them for the allocated resources. Based on the number of spectrum bands that each BS *k* won, it allocates an aggregated rate $r_{i,k}^{\text{agg}} = r_{i,k,n}^{t,\text{opt}} + r_{i,k}^{p,\text{opt}}$ to each UE - $\in \mathcal{K}_{\text{k}}$; that is, *n* is the number of winning spectrum bands for BS *k* from the spectrum auction.

Next, Lemma 4.3.1 shows how the *k*th BS price per unit bandwidth of the temporary resources (i.e., $p_{k,n}^{t}$ is negatively proportional with the maximum achievable rate of the *k*th BS from the temporary auctioned resources (i.e., $R_{k,n}^{t}$). Theorem 4.3.2 shows that the proposed bidding mechanism is a demand based one where the price per spectrum band, of the BS's bid, is not fixed but it is related to the BS's demand for additional resources.

Lemma 4.3.1 The price per unit bandwidth of the assigned temporary resources by BS *k* that is represented by the shadow price $p_{k,n}^{t}$ in Equation (4.6) [i.e., the Lagrangian of optimization problem (4.5)] is a strictly decreasing function with respect to $R_{k,n}^{t}$ (the maximum achievable rate of the *k*th BS) which indicates that the price per unit bandwidth of the temporary resources is negatively proportional with the maximum achievable rate $R_{k,n}^{t}$.

Proof Let $\sum_{i=1}^{|\mathcal{M}_k|} \log U_i(r_{i,k,n}^{t} + r_{i,k}^{p,\text{opt}})$, which is equivalent to the objective function in (4.5), be denoted by $f(\mathbf{r})$ where $\mathbf{r} = (r_{1,k,n}^{t}, r_{2,k,n}^{t}, \ldots, r_{|\mathcal{M}_k|,k,n}^{t})$ are the variables. Consider the problem of finding the maximum of $f(\mathbf{r})$ subject to the constraint $\sum_{i=1}^{|\mathcal{M}_k|} r_{i,k,n}^{t} + z_{k,n}^{t} = R_{k,n}^{t}$ with $\sum_{i=1}^{|\mathcal{M}_k|} r_{i,k,n}^{t} + z_{k,n}^{t}$ represented by $g(\mathbf{r}_{k,n}^{t})$.

Algorithm 4 The kth BS Optimal Bidding Algorithm

Receive application utility parameters β_i, a_i, b_i, and $r_i^{\max}$ from all UEs in $\mathcal{M}_k$.
Receive the number of auctioneer's spectrum bands N and the number of bidders K from the auctioneer.
Find the BS's assigned rates from its permanent resources R_k^p by solving
$\mathbf{r}_k^p = \arg\max_{\mathbf{r}_k^p} \sum_{i=1}^{|\mathcal{M}_k|} \log U_i(r_{i,k}^p) - p_k^p(\sum_{i=1}^{|\mathcal{M}_k|}(r_{i,k}^p) - R_k^p)$.
Let $r_{i,k}^{p,\text{opt}} = r_{i,k}^p \ \forall i \in \mathcal{M}_k$.
for $n = 1 \rightarrow N$ **do**
  Associate the number of spectrum bands n with a corresponding achievable rate $R_{k,n}^t$ {i.e., for each number of spectrum bands $n \in \mathcal{N}$ that BS k is bidding for.}
  Find the BS's assigned rates from the temporary resources $R_{k,n}^t$ by solving
  $\mathbf{r}_{k,n}^t = \arg\max_{\mathbf{r}_{k,n}^t} \sum_{i=1}^{|\mathcal{M}_k|} \log U_i(r_{i,k,n}^t + r_{i,k}^{p,\text{opt}}) - p_{k,n}^t(\sum_{i=1}^{|\mathcal{M}_k|}(r_{i,k,n}^t) - R_{k,n}^t)$.
  Let $r_{i,k,n}^{t,\text{opt}} = r_{i,k,n}^t \ \forall i \in \mathcal{M}_k$.
  for $j = 1 \rightarrow |\alpha|$ **do**
    if $\alpha_j(k) = n$ **then**
      Calculate $b_k(\alpha_j) = \sum_{l=1}^{n} D * p_{k,l}^t$.
    end if
  end for
end for
Create a bidding vector $\mathbf{b}_k = [b_k(\alpha_1), b_k(\alpha_2), \ldots]$.
Encrypt each bidding value in $\mathbf{b}_k$ and create an encrypted bidding vector $\hat{\mathbf{b}}_k$.
Submit the encrypted bidding vector $\hat{\mathbf{b}}_k$ to the secure gateway.

Let *R* and *k* be the short terms used for $R_{k,n}^t$ and $p_{k,n}^t$, respectively. For each choice of the parameter R, let **r***(R) of **r** be the values that maximize *f;* that is, **r*** = (r_1*, r_2*,..., $r|_{\mathcal{M}k}|$) and r^*_i is the solution of $p = S_i(r_i) = \frac{d \log U_i(r_i)}{dr_i}$. For logarithmic or sigmoidal-like utility functions $U_i(r_i)$ (recall utility function properties in Section 4.3.1), $r_i = S_i^{-1}(p)$ is strictly decreasing function and each solution r^*_i is equivalent to $S_i^{-1}(p^*)$. Then ***f (r*(R))*** is the maximum off for fixed value of the inputs *R*. The derivative

$$\frac{d}{dR} f(\mathbf{r}^*(R))$$

represents the rate of change in the optimal output from the change of parameter *R*.

Corresponding to **r*** (R) there is a value $p = p^*(R)$ such that they are a solution to the Lagrange multiplier problem (4.6), that is,

$$\nabla f(\mathbf{r}^*(R)) = p^*(R) \nabla g(\mathbf{r}^*(R))$$
$$R = g(\mathbf{r}^*(R))$$

where $r_i^* = R - \sum_{j,j\neq i}(r_j^*) = R - \sum_{j,j\neq i} S_j^{-1}(p^*)$. It follows that the following equation holds true

$$\begin{aligned} p^*(R) &= \frac{d}{dR} f(\mathbf{r}^*(R)) \\ &= \sum_{i=1}^{|\mathcal{M}_k|} \left(\frac{\partial}{\partial r_i^*} \left(f(\mathbf{r}^*(R)) \right) \frac{dr_i^*}{dR} \right) \\ &= \sum_{i=1}^{|\mathcal{M}_k|} \left(\frac{U_i'\left(r_{i,k}^{p,\mathrm{opt}} + r_i^*\right)}{U_i\left(r_{i,k}^{p,\mathrm{opt}} + r_i^*\right)} \right) \frac{dr_i^*}{dR} \end{aligned} \tag{4.8}$$

where the derivative in (4.8) is obtained by applying chain rule and $\frac{dr_i^*}{dR} > 0$. Therefore, the Lagrange multiplier is equivalent to the rate of the change in the optimal output $f(\mathbf{r}^*)$ resulting from the change of the parameter *R*. Next, we show that $p^*(R)$ is a decreasing function with *R*. For $p^*(R)$, we have the first derivative as

$$\frac{d}{dR}p^*(R) = \sum_{i=1}^{|\mathcal{M}_k|}\left(\frac{\partial}{\partial r_i}\left(\sum_{i=1}^{|\mathcal{M}_k|}\frac{U_i'\left(r_{i,k}^{p,\text{opt}}+r_i^*\right)}{U_i\left(r_{i,k}^{p,\text{opt}}+r_i^*\right)}\right)\frac{dr_i^*}{dR}\right)$$

$$= \sum_{i=1}^{|\mathcal{M}_k|}\left(\frac{U_i''\left(r_{i,k}^{p,\text{opt}}+r_i^*\right)U_i\left(r_{i,k}^{p,\text{opt}}+r_i^*\right)}{U_i^2\left(r_{i,k}^{p,\text{opt}}+r_i^*\right)}\right. \tag{4.9}$$

$$\left.-\frac{U_i'^2\left(r_{i,k}^{p,\text{opt}}+r_i^*\right)}{U_i^2\left(r_{i,k}^{p,\text{opt}}+r_i^*\right)}\right)\frac{dr_i^*}{dR}$$

where the derivative in (4.9) is obtained by applying chain rule. In the case of logarithmic utility function $U_i(r_{i,k}^{p,\text{opt}} + r_i^*)$, recall the utility function properties in Section 4.3.1, the utility function of the application rate is positive, increasing and twice differentiable with respect to the application rate. It follows that $U_i'(r_{i,k}^{p,\text{opt}} + r_i^*) = \frac{dU_i(r_{i,k}^{p,\text{opt}}+r_i^*)}{dr_i} > 0$ and $U_i''(r_{i,k}^{p,\text{opt}} + r_i^*) = \frac{d^2U_i(r_{i,k}^{p,\text{opt}}+r_i^*)}{dr_i} < 0$, that is, since $r_{i,k}^{p,\text{opt}} + r_i^*$ is greater than zero. Then the function $\log U_i(r_{i,k}^{p,\text{opt}} + r_i^*)$ has $\frac{d\log(U_i(r_{i,k}^{p,\text{opt}}+r_i^*)}{dr_i} = \frac{U_i'(r_{i,k}^{p,\text{opt}}+r_i^*)}{U_i(r_{i,k}^{p,\text{opt}}+r_i^*)} > 0$ and $\frac{d^2\log(U_i(r_{i,k}^{p,\text{opt}}+r_i^*)}{dr_i^2} = \frac{U_i''(r_{i,k}^{p,\text{opt}}+r_i^*)U_i(r_{i,k}^{p,\text{opt}}+r_i^*)-U_i'^2(r_{i,k}^{p,\text{opt}}+r_i^*)}{U_i^2(r_{i,k}^{p,\text{opt}}+r_i^*)} < 0$. On the other hand, in the case of

sigmoidal-like utility function, the normalized sigmoidal-like function is given by $U_i(r_{i,k}^{p,\text{opt}} + r_i^*) = c_i(\frac{1}{1+e^{-a_i(r_{i,k}^{p,\text{opt}}+r_i^*-b_i)}} - d_i)$. For $R > 0$, we have

sigmoidal-like utility function, the normalized sigmoidal-like function is given by $U_i(r_{i,k}^{p,\text{opt}} + r_i^*) = c_i(\frac{1}{1+e^{-a_i(r_{i,k}^{p,\text{opt}}+r_i^*-b_i)}} - d_i)$. For $R > 0$, we have

$$0 < c_i\left(\frac{1}{1+e^{-a_i\left(r_{i,k}^{p,\text{opt}}+r_i^*-b_i\right)}} - d_i\right) < 1$$

then,

$$0 < 1 - d_i\left(1+e^{-a_i\left(r_{i,k}^{p,\text{opt}}+r_i^*-b_i\right)}\right) < \frac{1}{1+c_id_i}$$

It follows that for R > 0, we have

$$\frac{d}{dr_i}\log U_i\left(r_{i,k}^{p,\text{opt}}+r_i^*\right)=$$

$$\frac{a_i d_i e^{-a_i\left(r_{i,k}^{p,\text{opt}}+r_i^*-b_i\right)}}{1-d_i\left(1+e^{-a_i\left(r_{i,k}^{p,\text{opt}}+r_i^*-b_i\right)}\right)}$$

$$+\frac{a_i e^{-a_i\left(r_{i,k}^{p,\text{opt}}+r_i^*-b_i\right)}}{\left(1+e^{-a_i\left(r_{i,k}^{p,\text{opt}}+r_i^*-b_i\right)}\right)}>0$$

$$\frac{d^2}{dr_i^{\,2}}\log U_i(r_{i,k}^{p,\text{opt}}+r_i^*)=$$

$$\frac{-a_i^2 d_i e^{-a_i\left(r_{i,k}^{p,\text{opt}}+r_i^*-b_i\right)}}{c_i\left(1-d_i\left(1+e^{-a\left(r_{i,k}^{p,\text{opt}}+r_i^*-b_i\right)}\right)\right)^2}$$

$$+\frac{-a_i^2 e^{-a_i\left(r_{i,k}^{p,\text{opt}}+r_i^*-b_i\right)}}{\left(1+e^{-a_i\left(r_{i,k}^{p,\text{opt}}+r_i^*-b_i\right)}\right)^2}<0$$

So, we have $\frac{d}{dR}p^*(R)=\frac{d^2}{dR^2}f(\mathbf{r}^*(R))<0$ where $f(\mathbf{r}^*(R))=\sum_{i=1}^{|\mathcal{M}_k|}\log U_i(r_{i,k}^{p,\text{opt}}+r_i^*)$ and each U_i is a logarithmic or sigmoidal utility function. Therefore, $p^*(R)$ is strictly decreasing function with R.

Theorem 4.3.2 By using the proposed bidding mechanism to determine the true bidding price of BS *k* for any allocation $\alpha_j \in \alpha$, for the bidding price $b_k(\alpha_j)$ of the $n = \alpha_j(k)$ spectrum bands where that price is determined by the summation of the price of each of the *n* spectrum bands [Equation (4.7)], the price of the *l*th spectrum band $(l \in \{1, 2, \ldots, n-1\})$ is greater than

the price of the (l + 1)th spectrum band; that is, $D * p^t_{k,1} > D * p^t_{k,2} > ... > D * p^t_{k,n}$. This indicates that the proposed bidding mechanism provide a demand-based bidding price as the bidding price per spectrum band is less when bidding for more spectrum bands.

Proof It follows from Lemma 4.3.1 that the price per unit bandwidth $p^t_{k,l}$ is a strictly decreasing function with $R^t_{k,l}$, where $l \in \{1, 2, \ldots, n\}$ and $R^t_{k,1} > R^t_{k,2} > \ldots > R^t_{k,n}$. Therefore, for certain number of spectrum bands n that BS k is bidding for, the price of the lth spectrum band, which is determined by $D * p^t_{k,l}$ is lower for larger l; that is, $D * p^t_{k,1} > D * p^t_{k,2} > \ldots > D * p^t_{k,n}$.

4.3.2 Spectrum Bands Allocation

The spectrum bands allocation procedure is similar to the one introduced in [198]. The auctioneer generates a private and public keys of Paillier cryptosystem and publishes his public key and element x (i.e., $x \neq 0$) over the pilot channel. Each bidder determines its true bidding values as shown in Section 4.3.1 and sends their encrypted values to the secure gateway, which creates an interference conflict graph for the bidders. The auctioneer selects a random BS to be the root BS and executes the spectrum auction in its subnet. The auctioneer then carries out the spectrum auction in the next subnet while excluding BSs that are previously considered root BSs along with the spectrum bands allocated to these BSs. The auctioneer continues to carry out the spectrum auction in one subnet after another until all BSs in $\mathcal{K}$ have participated in the auction. The secure gateway maintains a conflict table for each bidder as in [110]. After the execution of the spectrum auction in any subnet, the secure gateway updates the conflict tables of all bidders in that subnet.

In order to enable an efficient secure spectrum bands allocation, it is important to prevent an insincere auctioneer and greedy bidders from manipulating the auction. Bid-rigging between an insincere auctioneer and a greedy bidder can occur for the benefit of both if the auctioneer knows the bidding values and reveals the value of the winning bid to a greedy bidder. Fraud occurs when an insincere auctioneer overcharges the winner in order to increase his own profit. This result is an unexpected bad utility for the winner. To avoid possible bid-rigging and frauds, it is important to use an auction mechanism that allows the auctioneer to determine the winning BSs

and their payments without knowing their actual bidding values. In order to achieve this, we use a spectrum auction mechanism that leverages homomorphic encryption through Pailliar cryptosystem as in [198].

On the other hand, we adopt a payment method similar to the one used in Vickrey-Clarke-Groves (VCG) auction with Clarke pivot payments [225] as it satisfies the following desired economic properties: incentive compatibility, individual rationality, and no positive transfers as proved in [198]. By using this payment method, each winning bidder (i.e., bidder k is a winning bidder) is charged a price p_k that is equivalent to the difference between the social welfare with and without that bidder's participation. The charging price p_k is given by

$$p_k = \sum_{i \neq k} \hat{b}_i(\alpha^{*-k}) - \sum_{i \neq k} \hat{b}_i(\alpha^*) \qquad (4.10)$$

where allocation $\alpha^* = \arg\max_{\alpha \in \boldsymbol{\alpha}} \sum_i \hat{b}_i(\alpha)$ and allocation $\alpha^{*-k} = \arg\max_{\alpha \in \boldsymbol{\alpha}} \sum_{i \neq k} \hat{b}_i(\alpha)$.

The spectrum bands allocation procedure is presented as follows:

1. The secure gateway receives a sealed bidding vector $\hat{\mathbf{b}}_k$ from each BS k for its true bidding values of the allocations in α. We assume that the secure gateway is aware of which WSP each bidder belongs to. The secure gateway creates a conflict-table for each bidder, which contains all BSs within the interference range of that bidder with their allocated spectrum bands and charging price. The procedure of encrypting the bidding values using Paillier encryption is similar to the one presented in [198]. The secure gateway randomizes the bidding values and sends them to the auctioneer. For any bidder k, neither the auctioneer nor the other bidders know the actual bidding values of BS k.
2. The auctioneer selects a random bidder k as a root BS and considers its corresponding subnet. The auctioneer does not have an optimal choice for which subnet it starts running the auction from in order to maximize its profit.

3. The auctioneer runs a secure spectrum auction in the subnet of the current root BS *k* as presented in VI.C [198]. Once the auction results are revealed, the auctioneer determines the winning bidders and their charging prices.
4. Each winning BS is allocated its corresponding spectrum bands and is charged for the allocated resources. The secure gateway updates the conflict table of each winning BS with the allocated spectrum bands and their charging price. If all BSs in $\mathcal{K}$ have already been considered root BSs, the spectrum auction is considered complete and there is no need to proceed to the next step.
5. The auctioneer selects a new root BS *k*, that has not been considered as a root BS before, based on a random selection and considers its corresponding subnet, which consists of all BSs within the interference range of the root BS *k* that have not been previously considered as root BSs. The process is then repeated starting from Step 2.

The spectrum bands allocation process is summarized in Algorithm 5.

The computational complexity of the spectrum bands allocation algorithm is analyzed and compared to other secure spectrum auction algorithms. For a connected random graph with *K* nodes, the size of each subnet is in the order of $\mathcal{O}$(log K) [226]. For *N* spectrum bands available in a subnet, the number of possible allocations is $\binom{\log K+N-1}{N}$ The number of possible allocations by Stirling's formula is in the order of

$$\mathcal{O}\left(\frac{1}{\sqrt{2\pi N}}\left(1+\frac{N}{\log K-1}\right)^{\log K-\frac{1}{2}}\left(1+\frac{\log K-1}{N}\right)^{N}\right)$$

The computational complexity of our spectrum bands allocation algorithm is in the order of

$$\mathcal{O}\left(\frac{K\log K}{\sqrt{2\pi N}}\left(1+\frac{N}{\log K-1}\right)^{\log K-\frac{1}{2}}\left(1+\frac{\log K-1}{N}\right)^{N}\log K\right)$$

which is more efficient than the computational complexity of the allocation algorithm of the secure spectrum auction THEMIS in [126] that is in the order of $\mathcal{O}(K \log K (\log K)^N s \log K)$, where s is the number of possible bidding values.

Algorithm 5 Spectrum Bands Allocation Algorithm

Auctioneer creates a set of all bidders $\mathcal{K} = \mathcal{K}^1 \cup \mathcal{K}^2 \ldots \cup \mathcal{K}^L$
The secure gateway creates the interference conflict graph for BSs in $\mathcal{K}$ and a conflict table for each bidder
Auctioneer generates his private and public keys of Paillier cryptosystem and sends his public key along with element x to all BSs in $\mathcal{K}$
$\mathcal{K}_0 = \mathcal{K}$
Initialize $\beta = \phi$
while $\mathcal{K} != \phi$ **do**
  $k = random(\mathcal{K})$ {Auctioneer selects a random BS}
  $\mathcal{K}_k = include\_conflict(k)$ {Auctioneer creates a new subnet for root BS k by adding BSs that form its subnet from conflict table of that BS}
  $\beta_k = \mathcal{K}_k \cap \beta$ {β_k is set of previous root BSs in the subnet of root BS k}
  $\mathcal{K}_k = \mathcal{K}_k \setminus \beta_k$ {Auctioneer removes from $\mathcal{K}_k$ previous root BSs}
  $\mathcal{N}_k = \mathcal{N} \setminus \mathcal{N}_{\beta_k}$ {Auctioneer removes from $\mathcal{N}$ spectrum bands allocated to BSs in β_k}
  $\alpha_k = alloc\_vect(\mathcal{K}_k, \mathcal{N}_k)$ {Auctioneer forms allocation vector α_k and sends to $\mathcal{K}_k$}
  BSs $\in \mathcal{K}_k$ send encrypted bids to the secure gateway
  The secure gateway randomizes bids and sends them to auctioneer
  Auctioneer selects the highest allocation α^*
  Auctioneer charges price p_k to BS k
  $\mathcal{K} = \mathcal{K} \setminus \{k\}$
  $\beta = \beta \cap \{k\}$
  The secure gateway updates the conflict table for the winning BSs
end while

4.4 Numerical Results

In this section, we evaluate the performance of the proposed bidding mechanism for determining true bidding values that are used in a truthful and secure spectrum auction. We evaluate three performance metrics that need to be maximized in a successful spectrum auction. The considered performance metrics are spectrum utilization, auctioneer's revenue, and bidders' satisfaction.

We consider two cellular networks that belong to different WSPs located within the auctioneer's geographical region where a secure spectrum auction

is hosted in $X*Xm^2$ area by a broker who plays the role of an auctioneer. Each WSP has a number of BSs that decide to participate in the spectrum auction to obtain additional resources. We assume that each BS is located in the middle of the cellular cell such that UEs located within the BS's coverage area and belong to that BS's WSP are only allocated resources form that BS. Each active UE is running either real-time or delay-tolerant application [266-268]. We assume that each BS k has a permanent resource R_k^p that does not change while the auctioneer is running the spectrum auction. The BSs of the two WSPs are randomly placed in the auction's geographical area. We assume that any two BSs located within the interference range of each other cannot be allocated the same spectrum bands by the auctioneer. The interference range for each BS used in the simulations is determined based on the distance and is equivalent to 0.6X m. The auctioneer announces to all bidders the number of its spectrum bands N. We assume that one auctioned spectrum band consists of $D = 10$ units of bandwidth and that one spectrum band corresponds to an achievable rate that is equivalent to 10; that is, $R_{k,1}^t = 10$ corresponds to $n = 1$ auctioned spectrum band, $R_{k,2}^t = 20$ corresponds to $n = 2$ auctioned spectrum bands and so on. Each application running on the UE is represented by a sigmoidal or logarithmic utility function based on the application type [269, 270]. We use three normalized sigmoidal utility functions to represent real-time applications and three logarithmic utility functions to represent delay-tolerant applications. The used utility functions are shown in Figure 4.3 and their corresponding parameters are summarized in Table 4.2, where Sig1, Sig2, and Sig3 are approximations to VoIP, standard definition video streaming, and high-definition video streaming applications, respectively.

4.4.1 Bidding Prices and the Final Allocated Rates

In the following simulations, we consider 4 BSs (bidders) $\mathcal{K} = \{1,2,3,4\}$ participating in a secure and truthful spectrum auction. BS1 and BS2 belong to WSP1 (i.e., $\mathcal{K}^1 = \{1,2\}$) and BS3 and BS4 belong to WSP2 (i.e., $\mathcal{K}^2 = \{3,4\}$). The 4 BSs are demanding additional resources, and therefore they decide to participate in the spectrum auction. The permanent resources of the kth BS in $\mathcal{K} = \{1,2,3,4\}$ is as follows:

$R_1^p = 10, R_2^p = 20, R_3^p = 30,$ and $R_4^p = 40$. Each BS has 4 UEs under its coverage area subscribing for mobile services; that is, $\mathcal{M}^k$ = {1,2,3,4} is the set of active UEs for BS *k* where 1st UE in $\mathcal{M}^k$ is running real-time application represented by Sig2, the 2nd UE is running real-time application represented by Sig3, the 3rd UE is running delay-tolerant application represented by Log2, and the 4th UE is running delay-tolerant application represented by Log3. Algorithms 4 and 5 were applied in MATLAB for different number of auctioneer's spectrum bands $N \in \{1,2,..., 15\}$. Optimal bidding prices for all allocations in α are determined by each BS (bidder) after the execution of Algorithm 4. Additionally, after the execution of Algorithm 5 each BS is allocated its winning spectrum bands by the auctioneer and is charged the corresponding price.

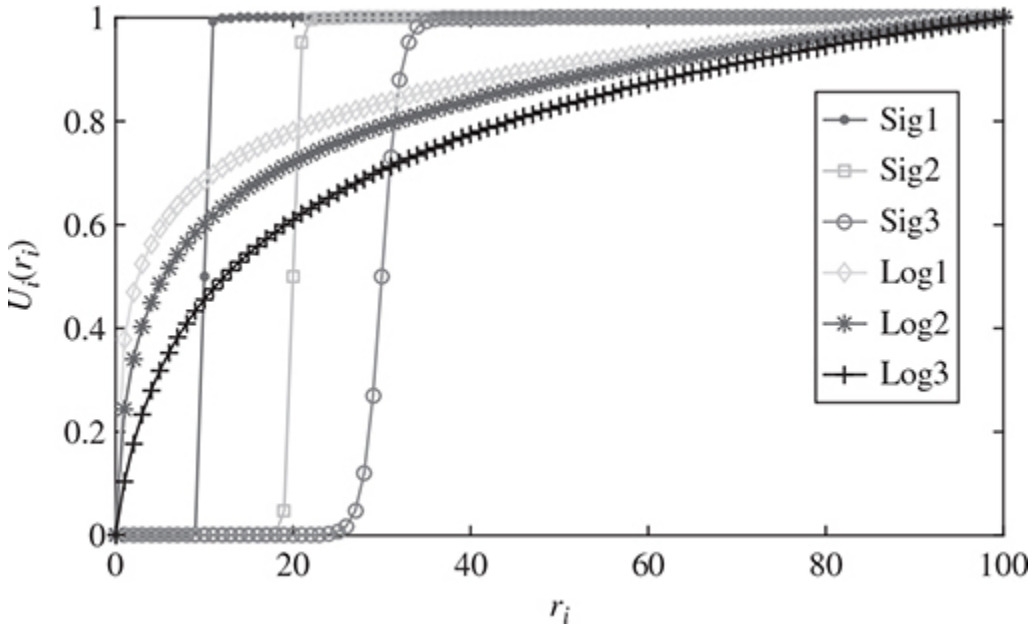


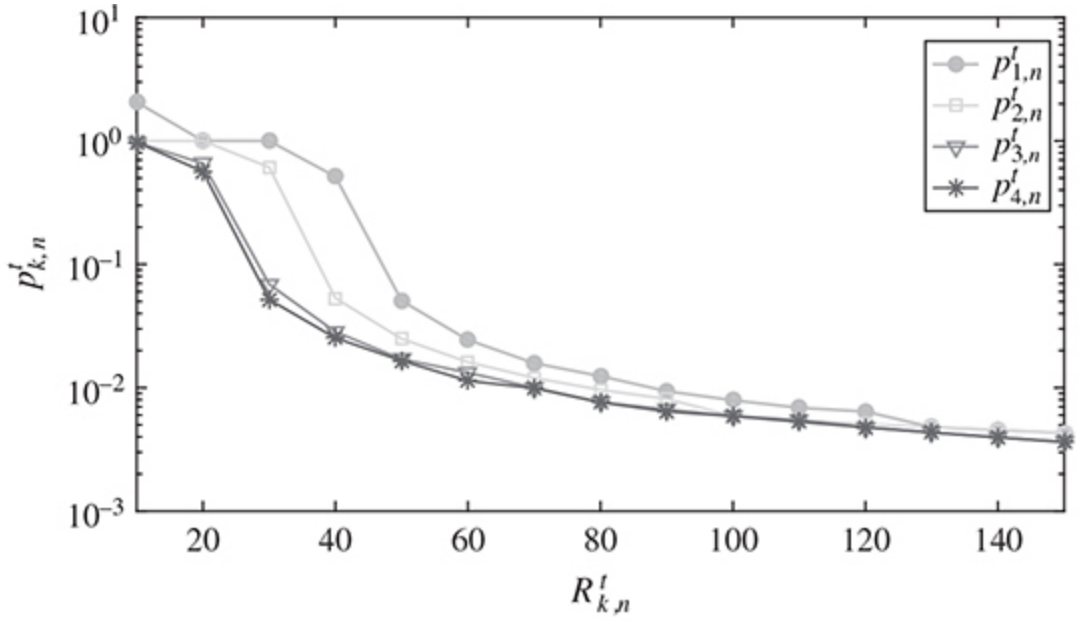
FIGURE 4.3 The users' utility functions $U_i(r_i)$ used in the simulation (three sigmoidal-like functions and three logarithmic functions).

Figure 4.4(a) shows each of the BS's shadow price (price per unit bandwidth) $p_{k,n}^t$ with the BS's temporary resources vary as $R_{k,n}^t$ = {10,20,30,..., 150}, which corresponds to *n* = {1,2,3,..., 15} auctioned spectrum bands. We notice that the BS's price per unit bandwidth is monotonically decreasing with $R_{k,n}^t$, that is, BS's shadow price for first

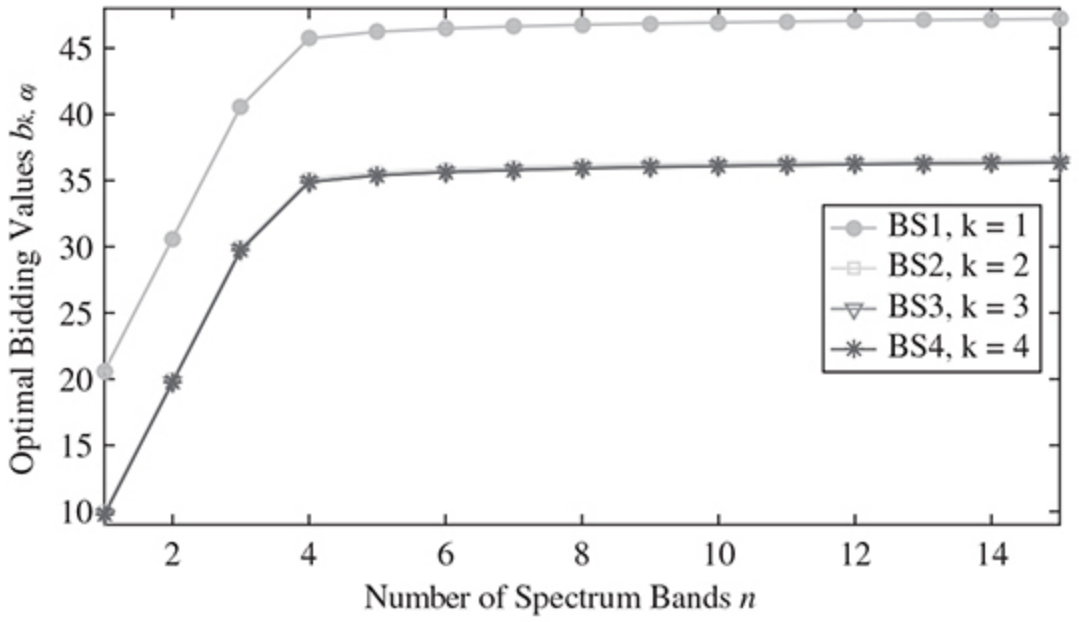
spectrum band is higher than second spectrum band and its price for the second spectrum band is higher than third spectrum band and so on, which is expected as the BS's demand for the lth spectrum band is higher than its demand for the (l + 1)th spectrum band. Figure 4.4(b) shows each BS's calculated bidding price $b_k(\alpha_j)$ for each number of spectrum bands n (i.e., $1 \leq n \leq 15$ and $\alpha_j(k) = n$) the BS is bidding for where $b_k(\alpha_j) = \sum_{l=1}^{n} 10 * p_{k,l}^t$ We observe that as the number of spectrum bands n increases, the BS's true bidding price increases. However, the increase in the bidding price is so minimal for higher number of spectrum bands n since the BS's demand for additional resources decreases.

Applications Utilities Parameters		Utility Function Type
Sig1	$a = 5,\ b = 10$	Sigmoidal Utility
Sig2	$a = 3,\ b = 20$	Sigmoidal Utility
Sig3	$a = 1,\ b = 30$	Sigmoidal Utility
Log1	$\beta = 15,\ r^{max} = 100$	Logarithmic Utility
Log2	$\beta = 3,\ r^{max} = 100$	Logarithmic Utility
Log3	$\beta = 0.5,\ r^{max} = 100$	Logarithmic Utility

TABLE 4.2 Users' Applications Utilities



(a) The shadow price $p^t_{k,n}$ for each of the 4 BSs (i.e., BS $k \in \{1,2,3,4\}$) with the BSs' temporary resources $10 \leq R^t_{k,n} \leq 150$.



(b) The 4 BSs' (bidders') optimal bidding values b_{k,α_j} with the number of spectrum bands each BS is bidding for, for example, $1 \leq n \leq 15$, for each of the 4 BSs (i.e., BS $k \in \{1,2,3,4\}$).

FIGURE 4.4 The 4 BSs (bidders) calculated shadow price with their temporary resources $10 \neq R^t_{k,n} \neq 150$ and the BSs optimal bidding values with the number of spectrum bands n each BS is bidding for; when the

permanent resources of BS1, BS2 BS3, and BS4 are $R_1^p = 10$, $R_2^p = 20$, $R_3^p = 30$, and $R_4^p = 40$ respectively.

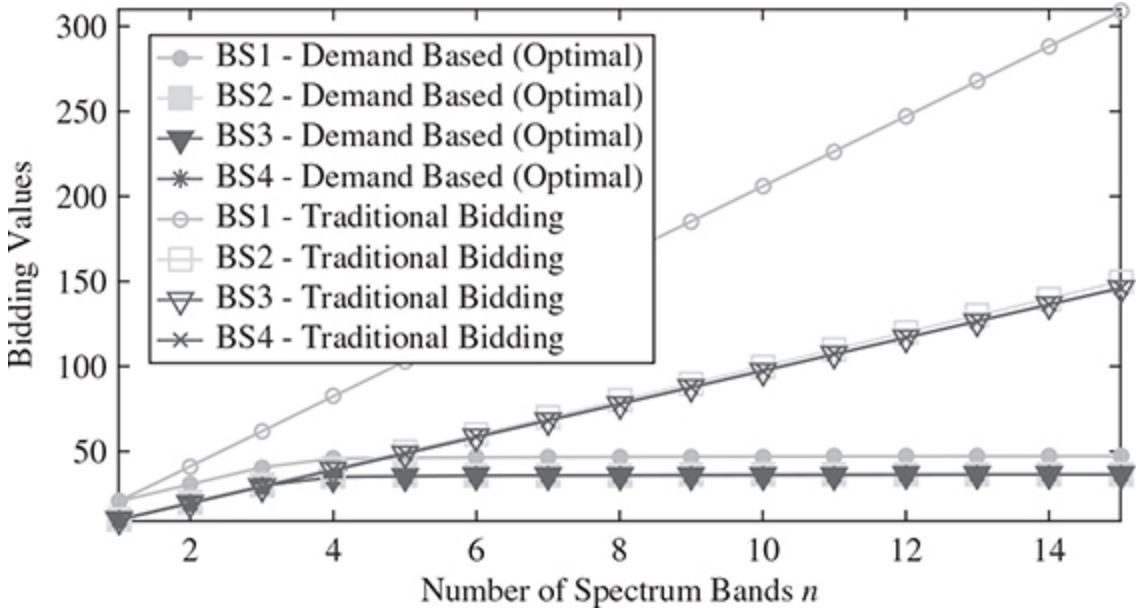
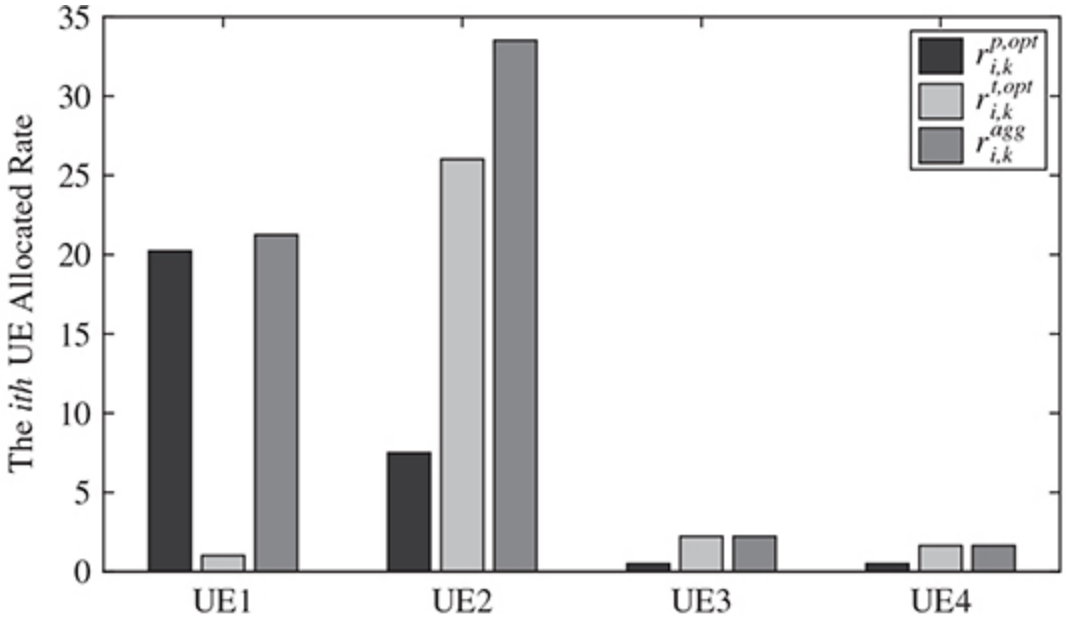


FIGURE 4.5 The bidding values obtained when using the proposed demand-based optimal bidding strategy compared to the bidding values obtained using a traditional bidding strategy, with the number of spectrum bands n that each BS is bidding for, for example, $1 \neq n \neq 15$, for each of the 4 BSs (bidders).

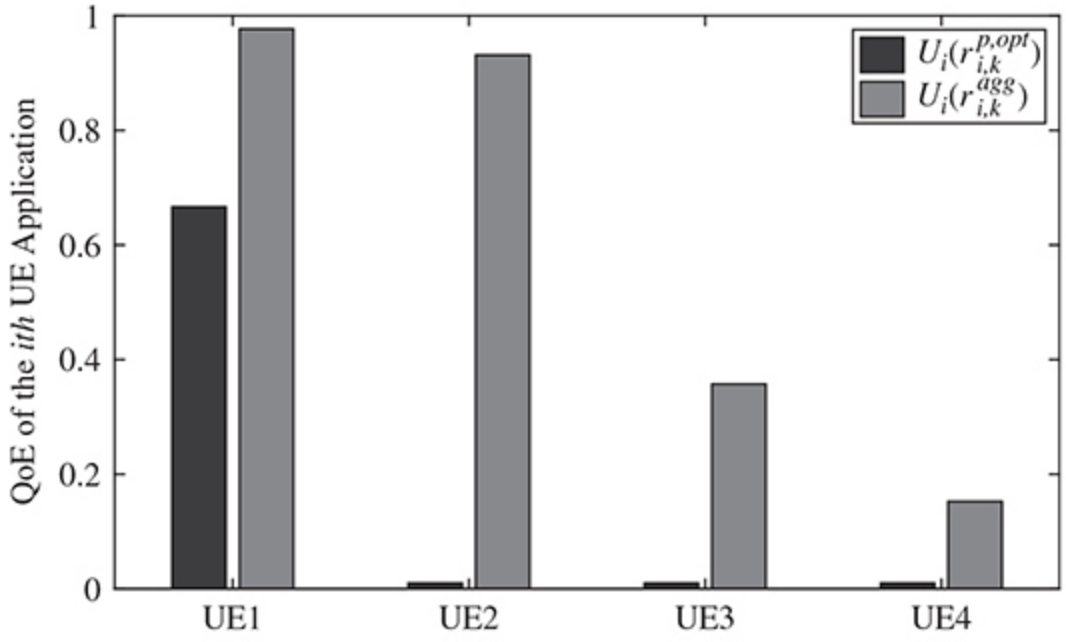
For the same simulation setup, we compare the BSs' bidding values obtained when using the proposed demand-based optimal bidding strategy with the bidding values obtained by a traditional bidding strategy. The bidding price per spectrum band when using a traditional bidding strategy is fixed, and therefore when a BS is bidding for a multiple of spectrum bands, the bidding price will be given by the price of one spectrum band multiplied by the number of spectrum bands the BS is bidding for. On the other hand, the price per spectrum band when using the demand-based approach varies based on the BS's demand of additional resources and the bidding price of each spectrum band is not fixed as explained throughout the section. Figure 4.5 compares the bidding price of the number of spectrum bands n, for example $1 \neq n \neq 15$, for each of the 4 BSs when using the proposed demand-based optimal bidding strategy and a traditional bidding strategy. We observe from Figure 4.5 how the bidding price does not continue to

grow after each BS reaches its required demand of additional resources when using the demand-based optimal bidding approach whereas when using a traditional bidding strategy, the bidding price continues to grow when bidding for more spectrum bands.

We ran Algorithms 4 and 5 in MATLAB for $N = 7$ spectrum bands and the number of each BS's winning spectrum bands is obtained as follows: BS1, BS2, BS3, and BS4 won 4, 4, 3, and 3 spectrum bands, respectively. Figure 4.6(a) shows BS3 allocated rates from its primary resources $R^{p}_{3} = 30$, temporary auctioned resources $R^{t}_{3,3} = 30$, and the aggregated final resources to each of the 4 active UEs under its coverage area. Figure 4.6(b) shows UEs' QoE represented by the UEs applications' utilities of their allocated rates from BS3. We notice that realtime applications are given priority when allocating the BS's resources due to the nature of their applications and the utility functions used to represent them, and none of the applications is allocated zero resources.



(a) BS3 optimal allocated rates $r_{i,3}^{p,opt}$, $r_{i,3}^{t,opt}$, $r_{i,3}^{agg}$ to each of the 4 UEs when BS3 permanent resources $R_3^p = 30$ and its winning auctioned resources is 3 spectrum bands (n = 4), which is equivalent to $R_{3,3}^t = 30$.



(b) BS3 users' QoE represented by the utility of user's application of its allocated rate $U_i(r_{i,k}^{p,opt})$, $U_i(r_{i,k}^{agg})$ when $R_3^p = 30$ and $R_{3,3}^t = 30$.

FIGURE 4.6 BS3 allocated rates to users under its coverage area and its users' QoE when $R^p{}_3 = 30$ and $R^t{}_{3,3} = 30$.

4.4.2 Performance Analysis

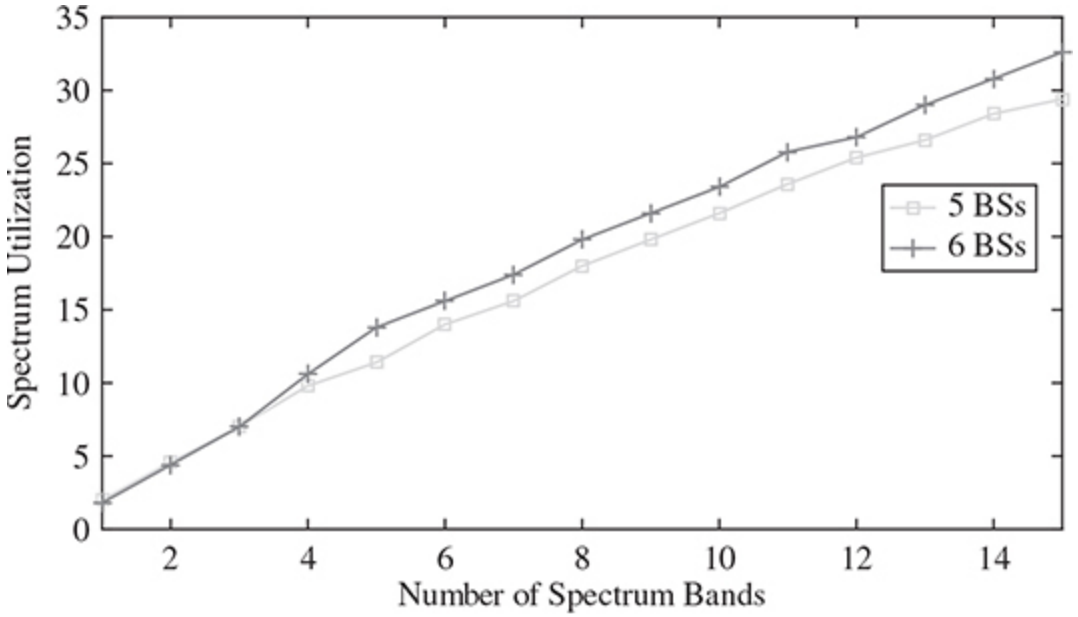
In the following simulations, we consider the network setup described above for 2 cases. In the first case, we considered 5 BSs (i.e., $\mathcal{K}$ = (1,2,3,4,5}) 3 of them belong to the first WSP and the other 2 belong to the second WSP with the k^{th} BS in $\mathcal{K}$has permanent resources $R_k^p = 10 * k$. In the second case, we considered 6 BSs (i.e., $\mathcal{K}$ = (1,2,3,4,5,6}): 3 of them belong to the first WSP and the other 3 belong to the second WSP with the kth BS in $\mathcal{K}$ has permanent resources $R^p{}_k = 10 * k$. We ran Monte Carlo simulation for the 2 cases and the results are averaged over 5 independent runs. In the 1st run, we consider 4 active UEs under the coverage area of each BS with each UE running one application that is selected randomly with a corresponding utility function equivalent to one of the utility functions shown in Figure 4.3. Similarly, in the 2nd, 3rd, 4th, and 5th run, we consider 6, 8,10, and 12 active UEs, respectively, under the coverage area of each BS with each UE running one application that is selected randomly with a corresponding utility function equivalent to one of the utility functions shown in Figure 4.3. Because of the difference in the number of active UEs and their applications, each run generated different bidding values. We observe the performance of the secure and truthful spectrum auction when using the proposed bidding strategy for the 2 cases with different number of spectrum bands N = (1,2,3,..., 15}.

We consider the three performance metrics listed and described below:

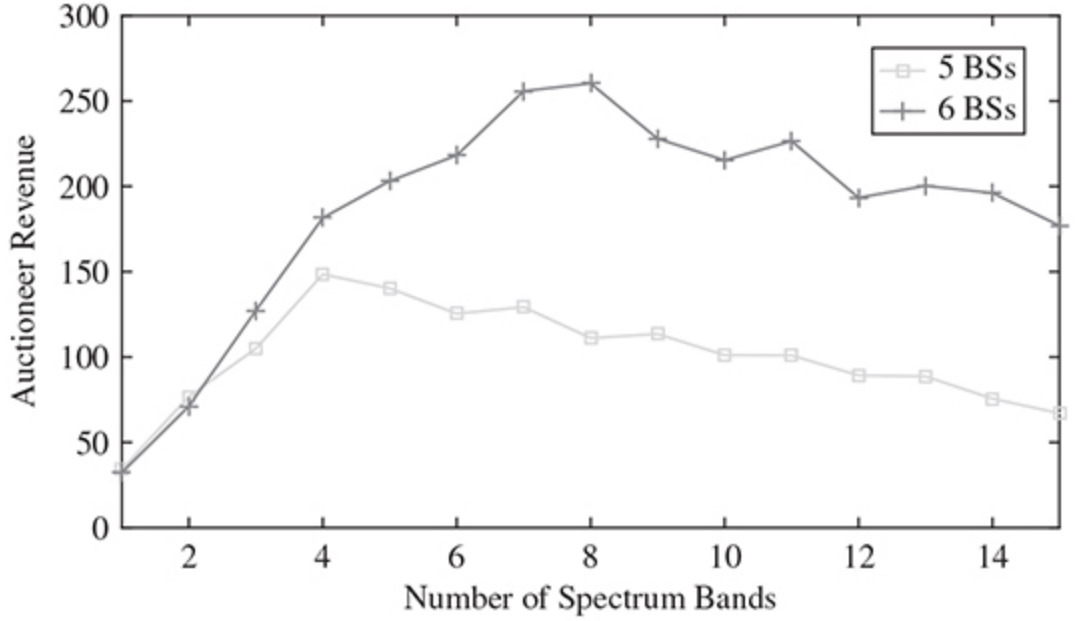
- Spectrum Utilization: It is represented by the sum of the spectrum bands that are allocated by the auctioneer to the winning bidders.
- Auctioneer's Revenue: It is given by the sum of all bidders; payments, that is, $Rev = \sum_{k=1}^{k=K} p_k$.
- Bidders' Satisfaction: It is represented by the sum of the utilities of all winning BSs divided by the sum of all bidders' evaluation values, that is, $\sum_{k\in\mathcal{W}} u_k / \sum_{k\in\mathcal{K}} e_k$, where $\mathcal{W}$ is the set of all winning BSs.

Figure 4.7(a) shows the spectrum utilization versus the number of the auctioneer's available underutilized spectrum bands. We observe that as the number of spectrum bands increases, the spectrum utilization, which is

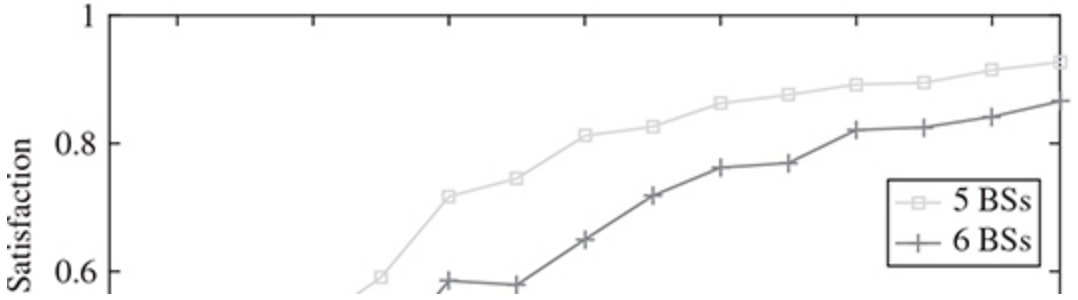
represented by the number of allocated spectrum bands, also increases. We also observe that for certain number of spectrum bands, the spectrum utilization is higher when the number of bidders increases. Figure 4.7(b) shows that the auctioneer's revenue increases when the number of BSs increases, which is expected as the auctioneer's revenue increases with more bidders requesting more spectrum bands. Figure 4.7(c) shows that as the number of spectrum bands increases, the bidders' satisfaction also increases until it saturates when each bidder is allocated the number of spectrum bands he bids for.

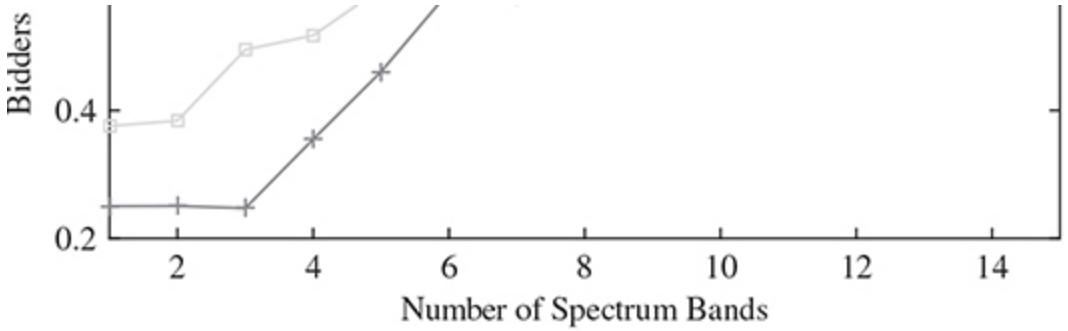


(a) Spectrum Utilization



(b) Auctioneer's Revenue





(c) Bidders' Satisfaction

FIGURE 4.7 Performance of the secure and truthful spectrum auction when using the proposed bidding mechanism.

4.5 Conclusion and Future Work

In this section, we proposed an optimal demand-based bidding mechanism to be used by BSs participating in a secure spectrum auction. The proposed mechanism allows each BS, with a demand for additional resources, to calculate its true bidding value for each number of spectrum bands it is bidding for. The proposed bidding strategy is ideal for a secure and truthful spectrum auction to guarantee truthfulness, which is a dominant strategy to prevent insincere behaviors of greedy bidders and an insincere auctioneer. We presented the BS's bidding algorithm, which is used to determine the BS's true bidding value that is based on the number of spectrum bands it is bidding for, the applications traffic of users under its coverage area, and the quantity of bidder's permanent resources. In addition, we proved that by using the proposed bidding mechanism, the biding price per each spectrum band is monotonically decreasing as the demand for each additional spectrum band decreases as the number of spectrum bands increases. We also presented a resource allocation based on carrier-aggregation approach to determine the BS's optimal aggregated rate allocated to each UE from both the BS's permanent resources and the BS's winning auctioned spectrum resources. Simulation results showed the performance of the proposed bidding mechanism when used in a secure spectrum auction. Our future work in spectrum auctions will consider designing a robust spectrum auction with heterogeneous spectrum bands. In cellular networks that have macro cells and micro/pico/femto cells, each bidder has different targeted cell coverage when bidding for spectrum bands; that is, macro cells' BSs

may favor low-frequency spectrum because of its long transmission range whereas femto cells' BSs would prefer high-frequency spectrum with transmission range that is enough for an indoor area. Future research work in spectrum auctions needs to take this into consideration.

---

[1]The content in this chapter is reproduced with permission after modifications (license number 4612590681390). For the original article, refer to [254].

CHAPTER 5

Secure Smart Grids Communications Using Homomorphic Encryption[1]

Haya Shajaiah, Ahmed Abdelhadi, and Charles Clancy

5.1 Introduction

In this chapter, we introduce a secure energy-trading auction approach to schedule the power plant limited resources during peak hours time slots. In the proposed auction model, the power plant serving a power grid shares with the smart meters (SMs) its available amount of resources that is expected during the next future peak time slot; SMs expecting a demand for additional power participate in the power auction by submitting bids of their offered price for their requested amount of power. In order to secure the power auction and protect SMs' privacy, homomorphic encryption through Paillier cryptosystem is used to secure the bidding values and ensure avoiding possible insincere behaviors of SMs or the grid operator (i.e., the auctioneer) to manipulate the auction for their own benefits. In addition, we use a payment rule that maximizes the power plant's revenue. We propose an efficient power scheduling mechanism to distribute the operator's limited resources among SMs participating in the power auction.

In this chapter, we design a secure power scheduling auction mechanism to schedule the power plant's limited electric power resources during peak hours time slots. The proposed mechanism allows the power grid operator to schedule his expected future available resources to the smart grids and charge them for the scheduled resources. It provides a framework for the power plant's operator, who plays the role of an auctioneer, to manage his

limited resources efficiently and securely. It uses homomorphic encryption to ensure users' privacy and secure the power auction, which is vulnerable to fraud of an insincere auctioneer and bid rigging.

5.2 System Model and Design Assumptions

We consider a power grid consisting of $\mathcal{K}$ SMs, denoted in the set $\mathcal{K}$ = (1,2,..., K}, that purchases electric power from a power plant operator (grid operator). We consider the situation where a set of SMs $\mathcal{N}$ = (1,2,., N}, $\mathcal{N} \subseteq \mathcal{K}$, are interested in purchasing additional amount of electric power (in addition to its regularly scheduled power) from the power plant operator to satisfy the demands of their commercial or industrial users during the next peak hours time slot. We express the power trading mechanism by designing a secure power auction. The grid operator plays the role of an auctioneer that auctions its spare resources to bidders (i.e., smart grids in $\mathcal{N}$). We assume that the grid operator is able to determine its expected amount of spare resources (electric power) denoted by *R* in KW that will be available during the next peak time slot. The amount of resources *R* is divided into *M* electric power units (EPUs). Let $\mathcal{M}$ = (1,2,...,M} denote the set of available EPUs to be auctioned by the grid operator to the *N* SMs in the power grid. We assume that the grid operator runs the power scheduling auction for future peak hours time slot during which a contingency will occur. Each SM can bid for a single or multiple EPUs from the set $\mathcal{M}$ based on its demand.

In the proposed power auction model, we consider a secure gateway that plays the role of a middleman between the auctioneer and the bidders. Figure 5.1 shows a power grid that consists of SMs, power plant, and secure gateway. The secure gateway announces to the SMs the number of bidders as well as the number of auctioned EPUs. Once the SMs receive these information, the interested SMs submit their bids (price) to the auctioneer.

Let $\mathcal{A}$ = {β^1, β^2,..., $\beta^{|\mathcal{A}|}$} be the set of all possible allocations for the *M* EPUs that each SM bids for and $|\mathcal{A}|$ is the number of all possible allocations. For example, in the case of $\mathcal{M}$ = (EPU1,EPU2} and $\mathcal{N}$ = (1,2,3}, then we have $\mathcal{A}$ = (β^1 = (2,0,0), β^2 = (0,2,0), β^3 = (0,0,2), β^4 = (1,1,0), β^5 = (1,0,1), and β^6 = (0,1,1)}, for example, β^1 = (2,0,0) denotes an allocation where EPU1 and EPU2 are scheduled for bidder 1 and nothing is

scheduled for bidder 2 and bidder 3. Each SM submits an encrypted bid for each allocation in $\mathcal{A}$ where $\mathbf{w_i} = [w_i(\beta^1), w_i(\beta^2),...]$ represents the encrypted bids that bidder i in $\mathcal{N}$ submits for the allocations in $\mathcal{A}$, for example, $\mathbf{w_2} = [0,2,0,1,0,1]$ indicates that SM 2 bids 0 for allocation β^1, 2 for allocation β^2, 0 for allocation β^3,1 for allocation β^4, 0 for allocation ft^5, and 1 for allocation ft^6. It is assumed that each SM submits same bids for different allocations in A if the number of EPUs that corresponds to that SM in these allocations is the same. The bidding values of each SM represent the price of the EPUs that the SM is bidding for. This price is traffic dependant [159]; that is, increases when the demand for more EPUs is high. Let $v_i(\beta)$ denotes the true evaluation value (bidding price) of SM i for allocation β and $\mathbf{v_i} = [v_i(\beta^1), v_i(\beta^2),...]$ be the true evaluation vector for SM i.

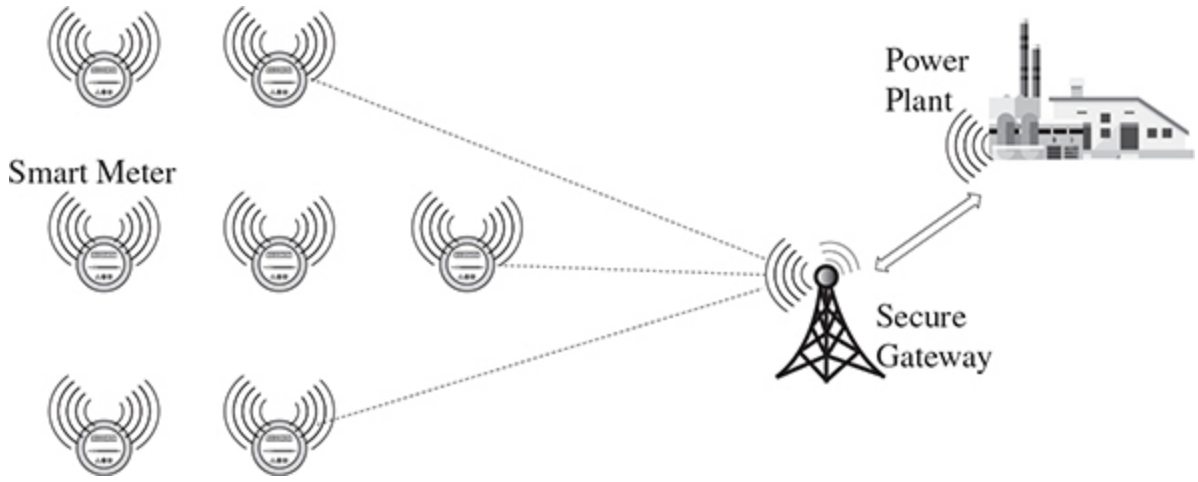


FIGURE 5.1 Power grid that consists of SMs, power plant, and secure gateway.

Let p_i denote the charging price of the auctioneer (grid operator) to SM i for the scheduled EPUs. Then the utility of SM i is given by $u_i = v_i(\beta) — p_i$; that is, the difference between the true evaluation value and the actual price that the SM pays to the auctioneer for allocation β. Furthermore, let $Rev = \sum_{i=1}^{i=N} p_i$ represent the power plant's revenue from selling the auctioned electric power R.

Providing an efficient contingency management using a secure power auction provides a fair scheduling mechanism and helps the grid operator improve its profit. It is important to take into consideration that the grid operator (auctioneer) is prone to fraud. Therefore, an ideal power auction should prevent possible backroom dealing by allowing the auctioneer to determine the winners and their payments, while the actual bidding values are kept secret from the auctioneer.

5.3 Design Considerations

In this section, we discuss some desired properties that are taken into consideration in the proposed power scheduling auction. First, we discuss the payment rule that the auctioneer adopts to determine the charging price that the SMs pay for the scheduled EPUs. Then we discuss the security and privacy challenges that need to be addressed in the auction design. Finally, we provide some background on homomorphic encryption.

5.3.1 Payment Rule

As mentioned before, our goal is to design a power scheduling auction that maximizes the power plant revenue. Therefore, we adopt the payment rule of Vickrey-Clarke-Groves (VCG) auction since VCG auction is proven to be Pareto efficient [224]. In order for an SM to maximize its utility, it has to bid with its true evaluation value regardless of the bidding strategies of other bidders [198]. In the proposed power auction design, we use a payment rule that is based on VCG auction mechanism [225] where each bidder is charged a price that is equivalent to the difference between the social welfare with and without that bidder's participation in the auction. Each SM *i* submits its encrypted bidding vector wj for the allocation set $\mathcal{A}$. Let $\beta^* \in \mathcal{A}$ be a Pareto-efficient allocation that the auctioneer selects where *3** is defined as

$$\beta^* = \arg\max_{\beta \in \mathcal{A}} \sum_i w_i(\beta) \tag{5.1}$$

The auctioneer schedules the EPUs in $\mathcal{M}$ to the SMs in $\mathcal{N}$ based on allocation β^*. Furthermore, let $\beta^*_{-i} \in \mathcal{A}$ be the allocation when SM *i* is

not participating in the auction that is defined as

$$\beta^*_{-i} = \arg\max_{\beta \in \mathcal{A}} \sum_{j \neq i} w_j(\beta) \tag{5.2}$$

The price that SM *i* is charged by the auctioneer for allocation β^* is equivalent

$$p_i = \sum_{j \neq i} w_j\left(\beta^*_{-i}\right) - \sum_{j \neq i} w_j(\beta^*) \tag{5.3}$$

Then the utility of SM *i* is $u_i = v_i(\beta^*) - p_i$. By using a VCG-based payment rule as expressed in Equation (5.3), many desired economic properties can be satisfied such as incentive compatibility, individual rationality, and no positive transfers (i.e., $p_i \geq 0 \forall i \in \mathcal{N}$) as proved in [198]. However, VCG auction cannot be directly used in the power scheduling auction because it is vulnerable to bid-rigging between the bidders and frauds of the insincere auctioneer.

5.3.2 Security and Privacy Considerations

One of the most important features of the proposed power scheduling auction is providing a sufficient level of security in order to enable a reliable and efficient scheduling of the auctioneer's resources. On the other hand, it is important to provide the SMs with a sufficient level of privacy by using a cryptosystem that allows bidders to submit their encrypted bidding values while keeping the actual values unknown to the auctioneer and other bidders in order to thwart backroom dealing such as bid-rigging between the bidders and the auctioneer and possible fraud of an insincere auctioneer. Bid-rigging can occur if the insincere auctioneer that is aware of the bidders actual bidding values colludes with certain bidder, for the benefit of both, by sharing with him the bidding values of other bidders and manipulate the auction. On the other hand, frauds of the insincere auctioneer occurs if the auctioneer manipulates the charging price and overcharges the winners in order to increase its revenue, which results in a bad utilities for the winners. Therefore, it is important for a power scheduling auction to use a

mechanism that allows the auctioneer to determine the maximum bid without knowing the actual bidding values.

5.3.3 Homomorphic Encryption

As mentioned before, homomorphic encryption is adopted in our auction design. Homomorphic encryption is used when there is a requirement to perform certain operations while the inputs are not disclosed. There are many schemes for homomorphic encryption. In the proposed auction design we adopt Pail-lier cryptosystem [212]. By using Paillier cryptosystem, the encryption function E(.) of plaintexts x_1 and x_2 is additively homomorphic, that is, $E(x_1 + x_2) = E(x_1)E(x_2)$. With the indistinguishability property of Paillier cryptosystem, if a plaintext x is encrypted twice the resulting two cyphertexts are different from each other, making it not possible for anyone to distinguish their original plaintexts unless decrypting the two ciphertexts. In addition, with the self-blinding property of Paillier cryptosystem, it is possible to compute different cipher-text $E'(x)$ from the ciphertext $E(x)$ without knowing the decryption key of the plaintext.

5.4 Secure Power Scheduling Auction Mechanism

Given that the grid operator who plays the role of an auctioneer could be a private entity, the auction is prone to fraud from an insincere auctioneer. Therefore, preventing possible insincere behavior from the auctioneer is essential. In order to enable an efficient secure scheduling process of the power plant's resources, it is important to design a secure power auction that enables the power plant's operator to determine the winners and the resource price without knowing the original bids. By making the auctioneer only able to exploit the winners and their payments, it is then not possible for him to conduct bid-rigging or fraud. Once the power auction is performed, the power plant's operator schedules each of the winning SMs for the corresponding EPUs and charges it for the scheduled resources. The proposed power auction leverages homomorphic encryption through Paillier cryptosystem to provide a secure and honest auction mechanism by avoiding possible frauds and bid-rigging. The procedure of the proposed secure power auction is presented in the following steps:

1. The auctioneer generates private and public keys of Paillier cryptosystem and shares his public key and element x (i.e., $x \neq 0$) with the SMs in the power grid.
2. Each SM i in $\mathcal{N}$ submits its true evaluation bidding values in $\boldsymbol{w(\beta)} = \boldsymbol{\beta}$ to a buffer that encrypts these values using Paillier cryptosystem and creates ciphertexts. The encrypted bids are then submitted to the secure gateway for randomization as described later in this section. For certain SM, let the bidding value $w(\beta)$ of allocation β be equivalent to m such that $1 \leq m \leq s$, where s is any number that is large enough to cover all possible bidding values for the allocation of the EPUs; that is, any actual bidding value does not exceed s. Let $E(x)$ be the Paillier encryption of the public element $x \neq 0$, the buffer creates a vector of ciphertexts $\boldsymbol{e}(m)$ for bidding value m, where $\boldsymbol{e}(m)$ is given by

$$\begin{aligned} \mathbf{e}(m) &= (e^1, \ldots, e^s) \\ &= (\underbrace{E(x), \ldots, E(x)}_{m}, \underbrace{E(0), \ldots, E(0)}_{s-m}) \end{aligned} \tag{5.4}$$

It is impossible to determine m without decrypting the elements in $\mathbf{e}(m)$ because of the self-blinding property of Paillier cryptosystem. The secure gateway randomizes the encrypted bids without knowing m. It adds a constant r to the encrypted vector **e**(m) and randomizes the rest of the elements. This results in the following vector

$$\mathbf{e}'(m+r) = (\underbrace{E(x), \ldots, E(x)}_{r}, e'_1, \ldots, e'_{s-r}) \tag{5.5}$$

The randomization is done without decrypting **e**(m) or knowing m. No information can be obtained, by the auctioneer, about the shifted amount r by comparing **e**(m) and **e**'(m + r) without decrypting both of them.

Furthermore, the auctioneer creates $N + 1$ representing vectors $\boldsymbol{E}_T$ = **E**(O), **E**i = **E**(O),...,En = **E**(O) (i.e., N is the number of bidders). The size of **E** equals $|A|$ and the initial $O(\beta)$ equals 0; that

is, **E**(O) = (e(0), e(0),..., e(0)}. Each SM; that is, the jth SM in $\mathcal{N}$ keeps its encrypted bidding vector **wj** secret by adding it to all representing vectors except E_j. Once performing this addition process by each SM in $\mathcal{N}$, the auctioneer obtains

$$\mathbf{E}_T = \left(\prod_i \mathbf{e}(w_i(\beta_1)), \ldots, \prod_i \mathbf{e}(w_i(\beta_{|\mathcal{A}|})) \right) \tag{5.6}$$

By applying the homomorphic addition property, $\mathbf{E}_T$ can be expressed as follows:

$$\mathbf{E}_T = \left(\mathbf{e}\left(\sum_i w_i(\beta_1) \right), \ldots, \mathbf{e}\left(\sum_i w_i(\beta_{|\mathcal{A}|}) \right) \right) = \mathbf{E}\left(\sum_i w_i \right) \tag{5.7}$$

and the auctioneer also has $\mathbf{E}_j = \mathbf{E}(\sum_{i \neq j} w_i)$ for $(1 \leq j \leq N)$.

3. The secure gateway adds a random constant $\theta(\beta) = r$ to each of $\mathbf{E_T}$, $\mathbf{E_1}$,..., $\mathbf{E_N}$ to obtain $\mathbf{E}(\sum_i w_i + \theta)$ and $\mathbf{E}(\sum_{i \neq j} w_i + \theta) \forall j$ and sends these randomized encrypted bids to the auctioneer.
4. The auctioneer determines the maximum sum value of the masked bids according to the following equation:

$$\begin{aligned} k &= \max_{\beta \in \mathcal{A}} \left(\sum_i w_i(\beta) + \theta(\beta) \right) \\ &= \max_{\beta \in \mathcal{A}} \left(\sum_i w_i(\beta) \right) + r \end{aligned} \tag{5.8}$$

where *k* can be determined by the auctioneer by taking the product of the

encrypted values in $\mathbf{E_T}$, which is equivalent to $\prod_{n=1}^{|\mathcal{A}|} \mathbf{e}(\sum_{i=1}^{N} w_i(\beta_n))$, and finding the maximum element in that product, which is equivalent to *k* in Equation (5.8).

5. The auctioneer decrypts the *k*th element of each vector $\mathbf{e}(\sum_i w_i(\beta) + \theta(\beta))$ in $\mathbf{E_T}$ for all the allocations in $\mathcal{A}$. Its decrypted value will be equivalent to zero or x. The allocation that has a decryption value equivalent to *x*, that is, *β** is the one that maximizes $\sum_i w_i$. The auctioneer considers *β** to be the winning allocation and schedules its resources to the corresponding SMs according to *β**.

6. In order for the auctioneer to find its charging price for each winning SM, the auctioneer decrypts $\mathbf{e}(\sum_{i \neq z} w_i(\beta^*) + \theta)$ of $\mathbf{E_z}$ (i.e., SM *z* is a winning one) and finds the value $(\sum_{i \neq z} w_i(\beta^*) + \theta)$. The auctioneer then finds the maximum value of the product of the encrypted elements $\max_{\beta \in \mathcal{A}}(\sum_{i \neq z} w_i(\beta) + r) = (\sum_{i \neq z} w_i(\alpha^*_{-z}) + r)$.

   The auctioneer calculates the charging price that each of the winning SMs needs to pay for the scheduled EPUs according to the following equation

$$p_z = \left(\sum_{i \neq z} w_i(\beta^*_{-z}) + r \right) - \left(\sum_{i \neq z} w_i(\beta^*) + r \right) \qquad (5.9)$$

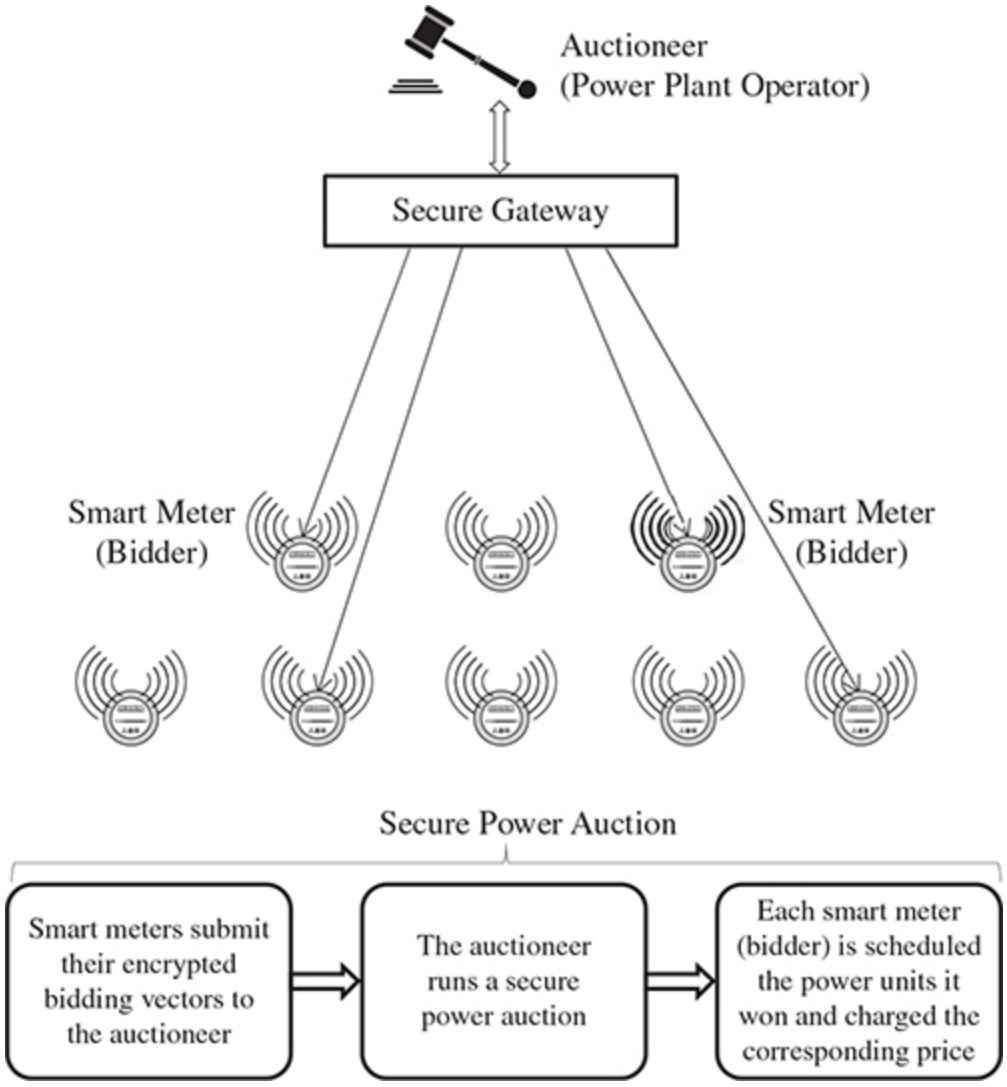

Auctioneer
(Power Plant Operator)
Secure Gateway
Smart Meter
(Bidder)
Smart Meter
(Bidder)
Secure Power Auction
Smart meters submit their encrypted bidding vectors to the auctioneer
The auctioneer runs a secure power auction
Each smart meter (bidder) is scheduled the power units it won and charged the corresponding price

FIGURE 5.2 Procedure of the proposed secure power scheduling auction.

where SM z is a winning bidder that pays a price p_z for its scheduled EPUs.

Figure 5.2 shows the procedure of the proposed secure power scheduling auction.

5.5 Numerical Results

In this section, we present through simulation results of the performance of the proposed power scheduling auction. Let $\mathcal{W}$ denotes the set of all winning SMs. Two performance metrics are considered:

- Power Plant's Revenue: The power plant's revenue *Rev* is given by the sum of all winning SMs' charging prices, that is expressed as *Rev* = $\sum_{i \in \mathcal{W}} p_i$
- Smart Meters' Satisfaction: It is represented by the sum of all winning SMs' utilities divided by the sum of all SMs' evaluation values that is given by $\sum_{i \in \mathcal{W}} u_i / \sum_{i \in \mathcal{N}} v_i$

These performance metrics need to be maximized in order to guarantee a successful power auction. In addition, we analyze the security and privacy procedure of the proposed power auction that ensures preventing any insincere behavior of the power plant operator or the SMs attempting to manipulate the auction.

We ran Monte Carlo simulation for different number of SMs that are bidding for the auctioneer's resources, and the results are averaged over the independent runs in which the bidding values of the SMs are generated randomly and the 2 performance metrics are evaluated. Simulation results are represented for each of the 4 cases: $N = 2$ SMs (bidders), $N = 3$ SMs, $N = 4$ SMs, and $N = 5$ SMs. We assume that there are no frauds or bid-rigging throughout the auctions. The simulation was run using MATLAB in Appendix B.

Figure 5.3 shows the auctioneer's revenue versus the number of EPUs for different number of bidders. We observe how the auctioneer's revenue increases when the number of SMs (bidders) increases. This is expected as the auctioneer's revenue increases with more bidders requesting more resources. Figure 5.4 shows that the bidders' satisfaction increases as the number of EPUs increases until the bidders' satisfaction saturates when each SM is assigned the number of EPUs it bids for. Figure 5.4 also shows that for the same amount of the auctioneer's available resources R, the bidders' satisfaction is higher when there are fewer bidders participating in the power auction.

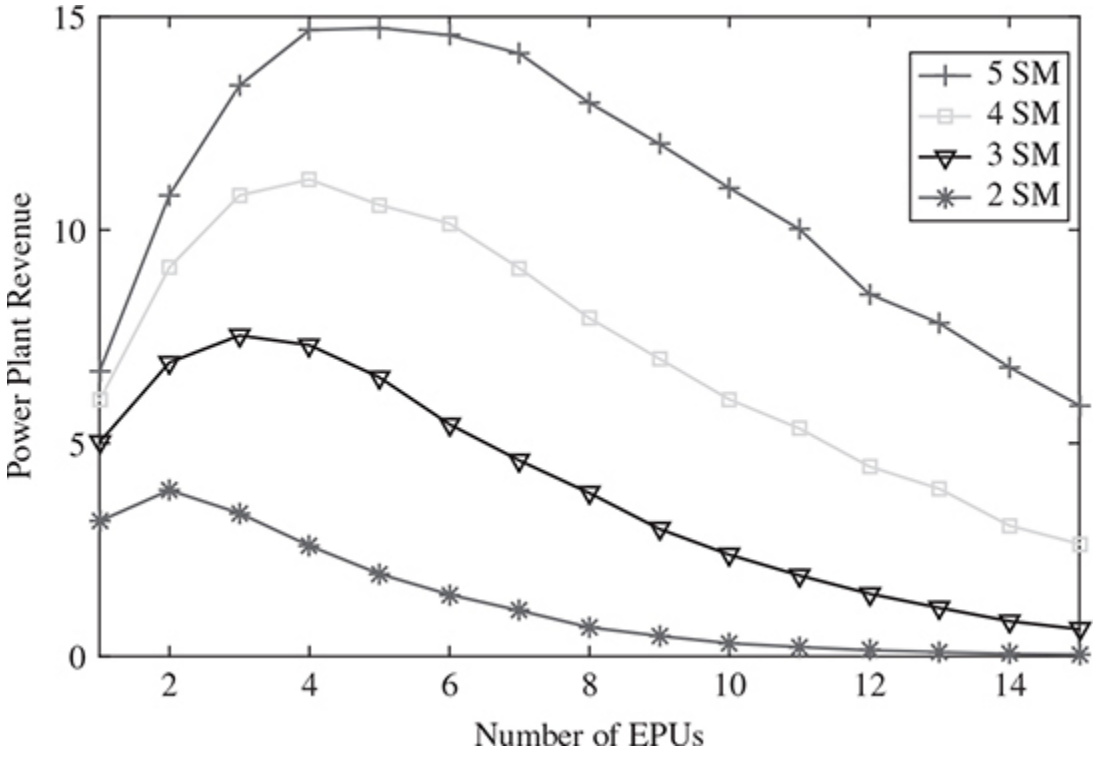


FIGURE 5.3 The auctioneer's revenue for different number of bidders with the auctioned EPUs changing from 1 to 15.

In addition to the satisfactory performance of the proposed power auction, it also guarantees security and privacy throughout the auction process. By using homomorphic encryption through Paillier cryptosystem, the SMs' bidding values remain unknown to the auctioneer while the auctioneer is still able to determine the winners and their charging price. With the indistinguishability property and the self-blinding property of Paillier cryptosystem, it is not possible to find the actual bidding value. We consider a secure gateway that plays an important role in securing the auction. The secure gateway randomizes the encrypted bids received from the SMs by a random constant r. Therefore, even if certain bidder colludes with the auctioneer, he cannot obtain any actual bidding value as the federal gateway randomized it. The auctioneer can then determine the winning SMs and their charging price without knowing the actual bidding values.

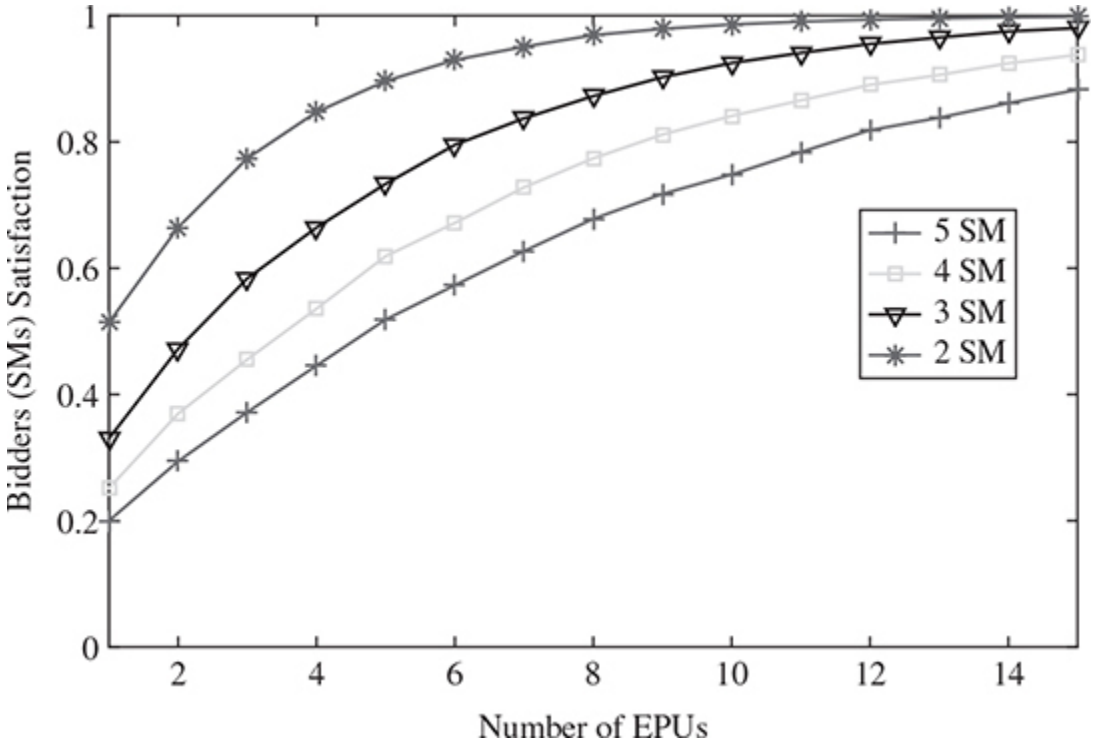


FIGURE 5.4 Bidders' satisfaction with the auctioned EPUs changing from 1 to 15.

5.6 Conclusion

In this chapter, we have proposed a secure power scheduling auction that enables an efficient power scheduling mechanism to schedule the power plant's limited resources during peak hours time slots. We have taken into consideration possible insincere behavior of the auctioneer and designed a power auction that prevents possible frauds and bid-rigging between an insincere auctioneer and greedy bidders. The proposed power auction leverages homomorphic encryption through Paillier cryptosystem to keep the SMs' bidding values unknown to the auctioneer, while the auctioneer is still able to find the winning SMs. We showed through simulations that the proposed power auction provides sufficient revenue for the power plant and satisfactory utilities for the SMs while providing a secure power scheduling auction against possible backroom dealings.

[1]The content in this chapter is reproduced with permission after modifications (license number 4612590595718). For the original article, refer to [271].

CHAPTER 6

Performance Trade-Offs in IoT Uplink Networks under Secrecy Constraints[1]

Haya Shajaiah, Avik Sengupta, Ahmed Abdelhadi, and Charles Clancy

6.1 Introduction

In this chapter, we investigate the performance of uplink communications in Internet of Things (IoT) networks under passive attacks from eavesdroppers capable of intercepting individual links. An industrial IoT network is studied where multiple sensor classes, each with a dedicated local access point (LAP), are connected to one or more small cell access points (SAP), which in turn are connected to a central server. The server interfaces the IoT network to industrial sensor monitoring systems, which periodically request sensor readings. We propose a unique attack-resilient IoT sensor reporting model and study the performance of this system under strict latency as well as secrecy constraints. We show through simulation results how the proposed model behaves in different scenarios and compare the resilience to attack capability for the different cases.

Uplink secrecy in IoT is very essential since the uplink communications contain data of potentially classified sensor reports. IoT security challenges and their potential solutions have been studied widely in previous research work such as in [187, 188]. However, these studies did not focus on the security of IoT uplink communication. In this work, we consider the uplink communication of latency-limited industrial IoT networks communicating critical sensor data. Since the communication of such time-sensitive critical

data over the IoT networks should ideally be of a confidential nature, the security of such data is an important design paradigm.

Recent works in [189,190] have studied secrecy in downlink networks. Conversely in this work, we present a latency-centric study of secrecy in latency-limited uplink IoT networks. We propose an attack-resilient system framework for sensor data reporting on the IoT uplink. Under passive attacks from an eavesdropper capable of intercepting transmissions on the uplink, we provide coun-termeasures to such attacks and study the cost of security in terms of latency and backhaul rate.

6.2 IoT Network Model

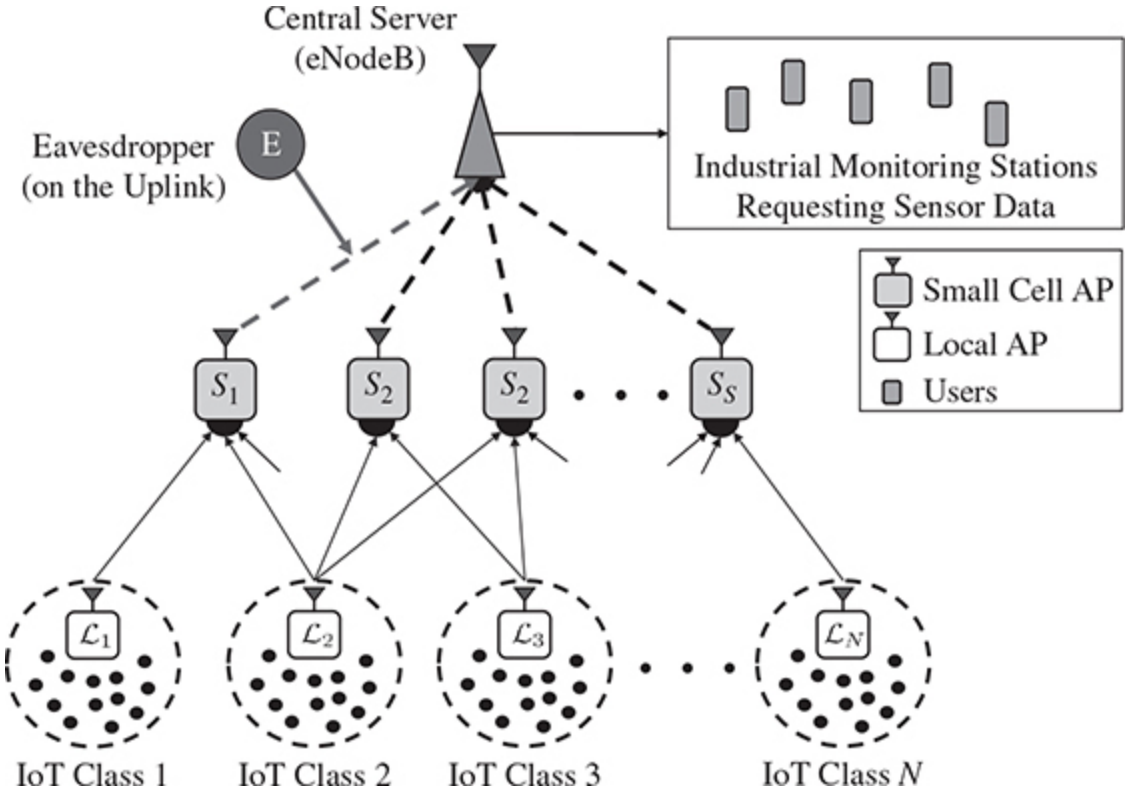


FIGURE 6.1 System model for uplink data communication in IoT.

We consider an IoT network where users (industrial monitoring stations) requesting data from different sensor classes form one edge of the network and the sensor classes form the opposite edge. The network model is illustrated in Figure 6.1. Under this setting, we consider data

communication from the sensors to the users over a potentially unsecure uplink.

6.2.1 Network Connectivity

We consider a set of N LAPs $\mathcal{L}_1, \mathcal{L}_2, ..., \mathcal{L}_N$. An IoT sensor class is a cluster of IoT sensors served by one LAP. Each LAP is connected to one or more SAPs. We assume that the IoT network has a total of S SAPs denoted by $\mathcal{S}_1, \mathcal{S}_2, ..., \mathcal{S}_S$. The connectivity between the LAPs and the SAPs is defined by a probabilistic coverage model, where probabilities $\gamma_{s,n}$ denote the probability of the SAP $\mathcal{S}_s$ being connected to the n—th IoT class LAP $\mathcal{L}_n$. We observe that

$$\sum_{n=1}^{N} \gamma_{s,n} = 1, \quad \forall s \in \{1, 2, \ldots, S\} \tag{6.1}$$

that is, the probability distribution is over the set of N sensor classes. Furthermore, note that the connection probabilities also account for physical layer characteristics of the network including fading, shadowing, and relative location (separation) of SAPs and LAPs. Equation (6.1) indicates that each SAP can be connected to one LAP at a time with $j_{S/n}$ being the average probability over multiple random realizations of the instantaneous network connectivity thereby accounting for topology/link changes over time. The set of SAPs is connected to a central server (e.g., an LTE eNodeB) through finite-capacity backhaul links. The server forms the gateway for the IoT sensor network to connect to the industrial monitoring stations, which request and track the sensor data. Thus, it is imperative that the central server is able to serve the monitors with their requested information with minimal latency. To this end, we next define the end-to-end communication policy on the uplink between the IoT LAPs and the central server.

6.2.2 Uplink Data Transmission Policy

In this work we concentrate on the IoT uplink model from the LAP to the central server in a latency-limited industrial setting where most sensor

readings have finite expiry times.

In order to incorporate the traffic characteristics of IoT networks, we assume that sensor reading requests from the industrial monitors are served directly from the central server with data already available in its buffer. We assume the server, being a central node, has a large enough buffer size to store reports from all N IoT classes under its service. Based on this assumption, it is pertinent to study the uplink data communication from the LAPs under varying latency constraints such that a *fresh set of sensor readings* is always available at the central server.

We next define the sensor reporting policy for the IoT network. The uplink communication policy is defined as $\pi = (\pi_E, \pi_F)$, where π_E is an *encoding policy* at the LAPs and π_F is a *forwarding policy* at the SAPs. The policies are designed to be resilient to eavesdroppers, and the associated protocols are defined next.

Encoding Policy π_E

The encoding of the sensor data for each IoT class is performed at the LAP for transmission to the SAPs serving them. To this end, we first define a composite sensor reading, namely the *sensor report*, SR_n at the LAP $\mathcal{L}_n$, which consists of readings from multiple sensors within the nth IoT sensor class. The monitors request these composite reports from the central server with the constraint that a fresh report be furnished on request. Each LAP collects data packets from its connected sensor nodes and encodes these packets using a rateless maximum distance separable (MDS) error correction code, such as raptor codes [273], which is proved to achieve linear time encoding and decoding complexity. Assume that each report SR_n is encoded into rateless coded packets such that *any* r packets suffice to decode the report at the central server. Similar to prior work in [5], we also assume that each report SR_n has an expiry time Δ_n, that is the time, from generation of the report, to the time at which it expires and is not valid for further use.

Forwarding Policy π_F

We next consider the action of the SAPs in the uplink policy. Each SAP, $\mathcal{S}_s$, $\forall s \in \{1, ..., S\}$, connects to the LAP $\mathcal{L}_n$, $\forall n$, with probability $\gamma_{s,n}$, to

retrieve at most r encoded packets from the LAP. Each SAP then aggregates and forwards the encoded packets to the central server with a transmit power budget of P. We define the fraction $m_{sn} \in [0,1]$ as the number of packets of SR_n retrieved by $\mathcal{S}_s$ normalized by the MDS parameter r. We define as t_n, the time taken by each SAP to process (retrieve, aggregate, and retransmit) a single packet from sensor class or LAP $n \in \{1, ..., N\}$ and forward to the central server. In our model, we allow for different processing times for different classes since, without loss of generality, each IoT class may use different radio access protocols, thereby requiring different times for processing and forwarding. In the case of a homogeneous radio access network, the times could be similar for all classes.[2] For example, if a SAP retrieves 5 packets from LAP $\mathcal{L}_1$, the delay in processing is $5t_1$. The processing time t_n is similar to a buffering time where the SAP collects all the packets and then transmits them together on the backhaul to the server. There is a *decodability constraint* at the central server such that it needs to receive at least r packets from each SR_n such that it can decode the messages for servicing monitor requests. The total processing time at each SAP is defined as follows:

$$T_p(s) = \sum_{n=1}^{N} m_{s,n}\, r\, t_n, \qquad \forall s \in \{1, \ldots, S\} \tag{6.2}$$

T_p (s) should be such that across all SAPs, the processing time is cumulatively large enough to process at least rN packets within the latency constraints. This is required due to the decodability constraint at the central server. Furthermore, an upper limit of T_p (s) can be the time taken to completely process all required rN packets at each SAP. Thus, we have

$$\frac{r}{S} \sum_{n=1}^{N} t_n \leq T_p(s) \leq r \sum_{n=1}^{N} t_n, \qquad \forall s \in \{1, \ldots, S\} \tag{6.3}$$

Subject to restrictions on Tp(s) related to the end-to-end latency, we consider the following: *what is the latency-optimal packet retrieval strategy for each SAP?* Since multiple SAPs can forward packets from the same

LAP, *transmission cooperation* at the SAPs is the main design goal. We aim to study such cooperation under passive attacks from an eavesdropper. To this end, we first define two different system frameworks and consequently address them under a threat model with counteractive secrecy constraints.

6.3 Latency-Centric IoT Uplink Framework

In this section, we present two frameworks that aid a latency-centric study of the IoT uplink. First, we consider a model where the backhaul links are rate-limited. Under this setting, we study the trade-off between the end-to-end latency of the system and the total processing time Tp(s) under fixed backhaul rate constraints. Secondly, we consider a latency-limited backhaul link with a fixed latency budget to maintain data freshness under varying backhaul rates. Under this setting, we study the trade-off between the backhaul rate and the total processing time *Tp(s)* under strict latency constraints. We next develop each framework separately.

6.3.1 Rate-Limited Backhaul Network

Consider a rate-limited backhaul link between each SAP and the central server with a fixed rate of log(P) bits/sec. The latency over these links for transferring data from the SAPs to the central server is then proportional to the amount of data, $m_{s,n}$, fetched by each SAP from their connected LAPs. Thus, the end-to-end latency[3] for each SAP can be written as:

$$\mathsf{L}(\mathsf{s}) = \sum_{n=1}^{N} r\, m_{s,n} \left(t_n + \frac{1}{\log(P)} \right) \tag{6.4}$$

Further, based on the coverage probability, $\gamma_{S,n}$, of the SAPs, we can write an expected end-to-end latency for each SAP as:

$$\mathsf{L}_{\mathsf{exp}}(\mathsf{s}) = \sum_{n=1}^{N} \gamma_{s,n}\, r\, m_{s,n} \left(t_n + \frac{1}{\log(P)} \right) \tag{6.5}$$

The expected latency is thereby dependent on the fraction of retrieved packets and their related processing times at the SAPs subject to a total

processing time constraint at each SAP. Further, the end-to-end decodability constraint dictates that the central server receives at least *r* packets from each sensor class. Finally, we define a parallel access protocol highlighting the method in which the central server accesses data from the SAPs. In this access protocol, the SAPs can send their data in parallel to the central server. As a result, the end-to-end latency of this system is limited by the maximum latency faced by any of the constituent SAPs.

We next formulate a joint optimization problem to minimize the end-to-end latency of the parallel access system. This problem entails the SAPs to jointly fetch content by accounting for the network topology. Let **M** be an $S \times N$ data retrieval matrix

$$\mathbf{M} = [m_{s,n}] = \begin{bmatrix} m_{1,1} & \dots & m_{1,N} \\ \vdots & \ddots & \vdots \\ m_{S,1} & \dots & m_{S,N} \end{bmatrix}$$

where $s = \{1,S\}$ and $n = \{1,N\}$. Then the minimum system latency can be expressed as the solution of the following minimization problem:

$$\underset{m_{s,n} \in \mathbf{M}}{\text{minimize}} \left[\max_{s \in 1,2,\dots,S} \sum_{n=1}^{N} \gamma_{s,n}\, r\, m_{s,n} \left(t_n + \frac{1}{\log(P)} \right) \right] \tag{6.6}$$

$$\text{subject to:} \quad \sum_{s=1}^{S} m_{s,n} \geq 1, \qquad \forall n \in 1,2,\dots,N \tag{6.7}$$

$$\sum_{n=1}^{N} r t_n m_{s,n} \leq T_p(s), \quad \forall s \in 1,2,\dots,S \tag{6.8}$$

Let the solution to the system be $L_{eX}p(opt)$. The minimization in (6.6) aims to minimize the worst case end-to-end latency in the system. The constraints (6.7)-(6.8) are explained as follows: The first constraint (6.7) follows directly from the decodability constraint of SR„ at the central server. The second constraint (6.8) is based on the per SAP processing time

constraint *Tp(s)*. This is an equivalence of the buffer processing time and enables the APs to fetch more content based on the allowable processing time. Finally, the formulation in (6.6)-(6.8) assumes that none of the sensor reports expire within the time taken for transmission under the constraint (6.8), that is, $\Delta_n \leq \min_{s\in 1,..,S} L_{exp}p(s)$. Note that Tp(s) and transmission power *P* are system parameters, which can be varied to study the latency performance. In this formulation we are interested in the L_{exp}(opt) versus *Tp* (s) trade-off. The optimization problem in (6.6) is based on minimizing the maximum of linear *S* linear terms. Thus, we can use linear programming (LP) to equivalently reformulate (6.6) by introducing an auxiliary variable L_{Aux}, as follows:

$$\underset{m_{s,n}\in \mathbf{M}}{\text{minimize}} \quad L_{Aux} \qquad \text{subject to:} \tag{6.9}$$

$$\sum_{n=1}^{N} \gamma_{s,n}\, r\, m_{s,n} \left(t_n + \frac{1}{\log(P)} \right) \leq L_{Aux}, \quad \forall s \tag{6.10}$$

in addition to constraints (6.7)-(6.8). The problem in (6.9) is a linear program subject to linear constraints and hence can be solved numerically.

6.3.2 Latency-Limited Backhaul Network

Consider a latency-limited backhaul network, where the link between each SAP and the central server is not rate limited but is limited by a total latency constraint. In this setting, we consider a total latency constraint T_{total} such that

$$T_{\text{total}} \geq T_p(s) + T_b(s), \qquad \forall s \in 1, \ldots, S \tag{6.11}$$

where T_b(s) is the latency on the backhaul link from $\mathcal{S}_n$ to the central server. Further, we have $\Delta_n \leq T_{total}$, that is, the latency constraint ensures data freshness at the central server. Based on amount of data downloaded by each SAP, the rate of the backhaul transmission varies since the link has fixed latency. The backhaul rate due to each SAP can be expressed as

$$\mathsf{R(s)} = \frac{\sum_{n=1}^{N} r\, m_{s,n}}{T_{\text{total}} - T_p(s)} \ \text{packets/unit time} \tag{6.12}$$

Thus, under probabilistic connectivity model, the expected backhaul rate can be expressed as

$$\mathsf{R}_{\text{exp}} = \sum_{s=1}^{S} \frac{\sum_{n=1}^{N} r\, \gamma_{s,n}\, m_{s,n}}{T_{\text{total}} - T_p(s)} \tag{6.13}$$

Again, an optimization problem similar to (6.6) can be formulated to minimize the expected backhaul rate

$$\underset{m_{s,n} \in \mathbf{M}}{\text{minimize}} \quad \mathsf{R}_{\text{exp}} \tag{6.14}$$

$$\text{subject to:} \quad \sum_{s=1}^{S} m_{s,n} \geq 1, \qquad \forall n \in 1, \ldots, N \tag{6.15}$$

$$\sum_{n=1}^{N} r t_n m_{s,n} \leq T_p(s), \quad \forall s \in 1, \ldots, S \tag{6.16}$$

$$T_{\text{total}} \geq T_p(s) + T_b(s), \quad \forall s \in 1, \ldots, S \tag{6.17}$$

Similar to the previous framework, (6.14) is a linear program which can be solved numerically. In this setting, we are interested in the optimal expected backhaul rate versus processing time, that is, $R_{eX}p(opt)$ versus $T_p(s)$ trade-off. We next look at the attack models in the IoT network in the presence of an eavesdropper.

6.4 Secrecy in IoT: Attack Models

Uplink secrecy in IoT is an important paradigm since the uplink data communication consists of potentially classified sensor reports SR_n, Vn. Therefore, a main design goal of the proposed system is resilience against

unauthorized access. To this end, we study a passive eavesdropper-based attack model and related secrecy constraints under which the eavesdropper is incapacitated. The proposed MDS coding of sensor reports acts as a means of adding redundancy to aid robustness against passive eavesdroppers and leads to simpler countermeasures for absolute secrecy.

6.4.1 Passive Eavesdropping on the Backhaul Link

In this attack model (illustrated in Figure 6.1), an eavesdropper, E, is capable of observing and intercepting uplink transmissions on one or more SAP-eNodeB links. From an eavesdropper's perspective, data interception on such links is more rewarding than the LAP-SAP links since these links form the network bottleneck through which all N reports must pass. However, the SAP and eNodeB are unaware of which link is intercepted but are aware only of the number of links which can be attacked. Thus, to achieve secrecy over potentially compromised links, the SAP needs to ensure that r packets from any one sensor are never transmitted over the compromised links. Let B_c be the set of attacked links. If the eavesdropper is capable of intercepting transmissions on any $k \leq S$ links, then we have the cardinality of the set

$$|\mathcal{B}_c| = \binom{S}{k} \text{ backhaul links}$$

Thus, in order to ensure that the eavesdropper does not decode any sensor report with a passive attack on links in the set B_c, we have the following simple secrecy constraint:

$$\sum_{\ell \in \mathcal{B}_c} m_{\ell,n} < 1, \quad \forall n \in 1, \ldots, N \tag{6.18}$$

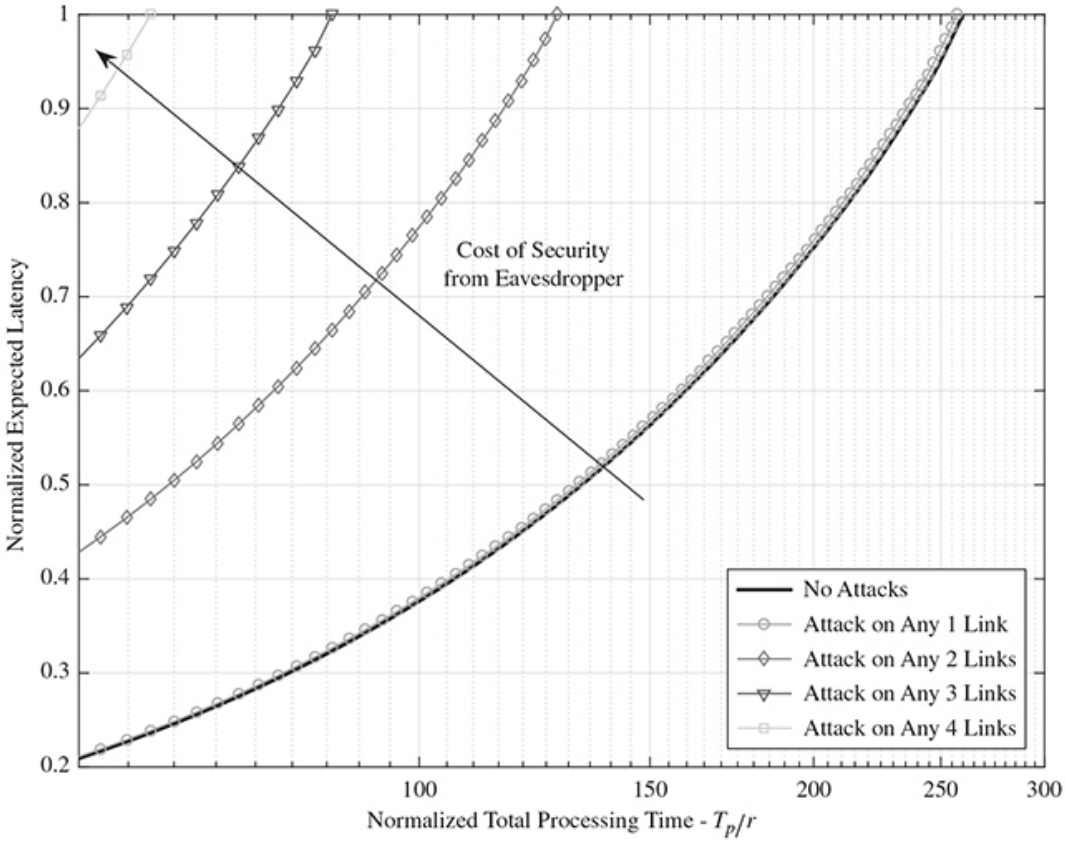
Note that the constraint (6.18) takes a simple form due to the attack-resilient design of the system model. Solving the linear programs (6.9) and (6.14) subject to the additional constraint (6.18) entails a latency-centric study of secrecy from an eavesdropper in the IoT uplink network.

6.5 Numerical Results

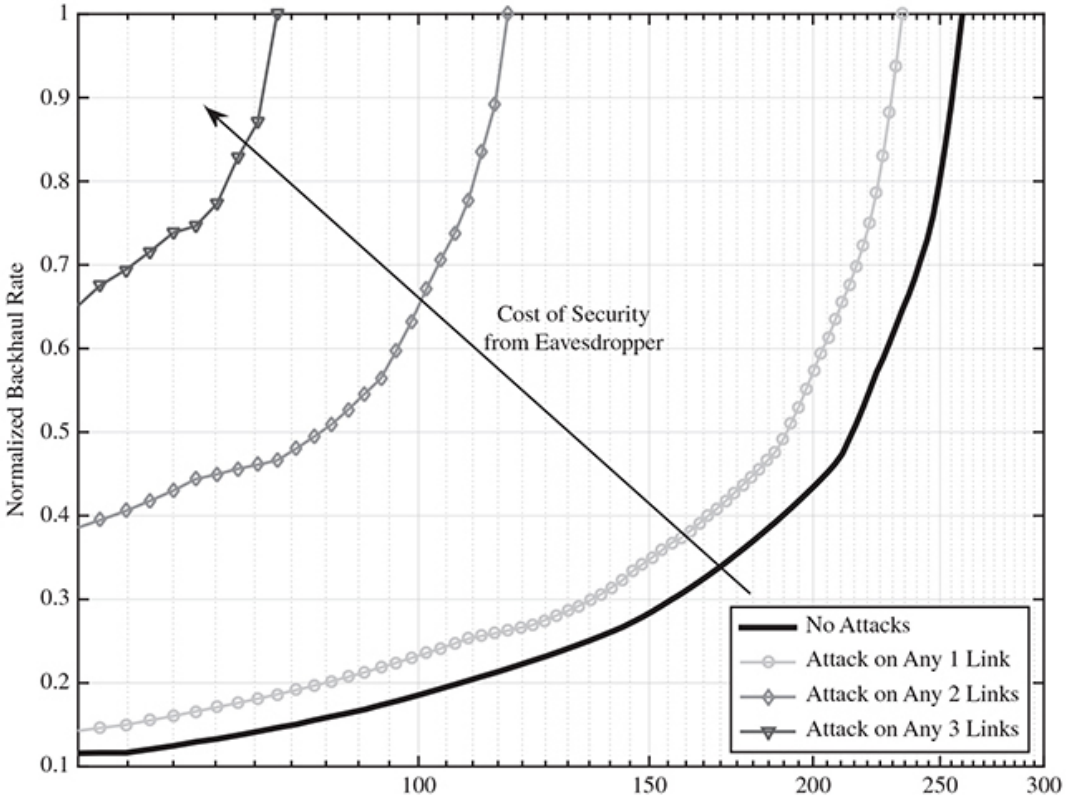
In this section, we provide more insight into the uplink IoT network transmission under secrecy constraints for a network with $N = 52$ IoT classes and $S = 5$ SAPs. The network connectivity probabilities $7_{s,n}$ are generated according to a Zipf power law distribution with random exponents chosen uniformly between 0.25-0.5. This was chosen to model distance-based connectivity and a more intricate modeling is left as a direction for future work. We assume that the constraint *Tp* (s) is equal for each SAP and is varied between the limits in (6.3) to study the trade-offs. The number of packets *r* is a system parameter and as a result, we choose *r* t_n uniformly at random from the set {1,3,7,9} time units.

Figure 6.2(a) shows the expected latency versus processing time trade-off for the rate-limited backhaul framework under different attacks from an eavesdropper. The expected latency is normalized such that it is in the range [0,1] and both axes are further normalized by r. It can be seen that for the rate-limited links in absence of strong latency constraints, the effect of attacks is smaller. Even when 4 out of 5 links are attacked, a feasible solution still exists for tighter processing time constraints. The effect of a single link attack is almost negligible.

On the other hand, for the latency-limited backhaul network with total latency constraint, T_{to}tai, Figure 6.2(b) shows the normalized expected backhaul-rate versus processing time trade-off. In this case, we set the minimum allowed backhaul latency $T_b^{\min} = (\sum_{n=1}^{N} r\ t_n)/S$ while the total latency constraint is set as $T_{\text{total}} = 2(\sum_{n=1}^{N} r\ t_n + T_b^{\min})$. A more detailed study of the parametrization is undertaken in the journal extension of the current work. Under the stricter constraints, we see that attacks on the backhaul links have a much more pronounced effect and a feasible solution ceases to exist when 4 links are attacked.


Normalized Expreceted Latency
Normalized Total Processing Time - T_p/r
Cost of Security
from Eavesdropper
No Attacks
Attack on Any 1 Link
Attack on Any 2 Links
Attack on Any 3 Links
Attack on Any 4 Links
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
100
150
200
250
300

(a)


Normalized Backhaul Rate
Cost of Security
from Eavesdropper
No Attacks
Attack on Any 1 Link
Attack on Any 2 Links
Attack on Any 3 Links
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
100
150
200
250
300

(b)

FIGURE 6.2 Passive attack by an eavesdropper on (a) rate-limited backhaul link and (b) latency-limited backhaul link.

The problem is infeasible for high Tp, which implies a very low T_b (since total latency is fixed) thereby increasing the rate. As attacks increase, reliable transmission cannot be achieved under the T budget for the backhaul links.

6.6 Conclusion

In this chapter, we presented a preliminary latency-centric study of an industrial IoT uplink network with latency-limited data communication under passive attack from an eavesdropper. We showed that under rate-limited backhaul links, the resilience to attacks on multiple links is better. For latency-limited backhaul links, the cost of security in terms of rate is relatively high, especially for a small number of attacked links. Future work in this paradigm will account for additional countermeasures for passive attacks such that secrecy can be achieved at a potentially lower cost. Furthermore, *active attacks from IoT classes* will be considered where rogue LAPs can flood the SAP with spurious packets, thereby crippling the network. The methods developed in this work can be extended to include other networks such as vehicular networks [274], multicast networks [275, 276], and other wireless networks [277-281].

[1]The content in this chapter is reproduced with permission after modifications (license number 4761470430584). For the original article, refer to [272].

[2]Note that for a multi-RAT (radio access technology) scenario, the SAP will need to be equipped with the capability to receive on different RATs on the uplink and then use LTE on the backhaul link to the server for transmitting the aggregated packets.

[3]We assume that the SAPs aggregate data from each LAP at a fixed latency and that the LAP-SAP links are not rate limited. Thus, we do not account

for this latency in the formulation choosing instead to adjust the Tp(s) accordingly to account for it.

CHAPTER 7

Securing Machine-to-Machine Uplink Communications[1]

Akshay Kumar, Ahmed Abdelhadi, and Charles Clancy

7.1 Introduction

Machine-to-machine (M2M) networks, being connected to the Internet at large, inherit all the cyber-vulnerabilities of the standard information technology (IT) systems [283, 284]. Since perfect cyber-security and robustness is an idealistic construct, it is worthwhile to design intrusion detection schemes to quickly detect and mitigate the harmful consequences of cyber-attacks. Volumetric anomaly detection has been popularized due to their low complexity, but they cannot detect low-volume sophisticated attacks and also suffer from high false-alarm rate. To overcome these limitations, feature-based detection schemes have been studied for IT networks. However, these schemes cannot be easily adapted to M2M systems due to the fundamental architectural and functional differences between the M2M and IT systems. In this chapter, we propose novel feature-based detection schemes for a general M2M uplink to detect distributed denial-of-service (DDoS) attacks, emergency scenarios, and terminal device failures. The detection for DDoS attack and emergency scenarios involves building up a database of legitimate M2M connections during a training phase and then flagging the new M2M connections as anomalies during the evaluation phase. To distinguish between DDoS attack and emergency scenarios that yield similar signatures for anomaly detection schemes, we propose a modified Canberra distance (MCD) metric. It

basically measures the similarity or differences in the characteristics of interarrival time epochs for any two anomalous streams. We detect device failures by inspecting for the decrease in active M2M connections over a reasonably large time interval. Lastly, using Monte Carlo simulations, we show that the proposed anomaly detection schemes have high detection performance and low false-alarm rate.

Novel detection schemes are proposed to overcome the limitation of volumetric detection schemes. The proposed schemes are capable of detecting DDoS attacks, emergency scenarios, and terminal device failures in M2M applications. A modified Canberra distance metric is proposed to distinguish between emergency scenarios and DDoS attack in the case of similar signatures for anomaly detection schemes. The proposed approach allows detection of device failures by inspecting for the decrease in active M2M connections over a large time interval. Simulation results show that the proposed anomaly detection schemes have high detection performance and low false-alarm rate.

7.2 System Model

Figure 7.1 shows the anomaly detection framework for a general M2M system [283-285]. The uplink traffic from each local group of terminal devices is first aggregated at an M2M aggregator (MA) and then the aggregated traffic from all MAs is processed at the M2M application server (AS). We assume the aggregated traffic at each MA follows a Poisson arrival process. Similar assumptions have been made in earlier work [286]. While the aggregated data at MAs usually consists of legitimate packets from the sensors, occasionally it may include fraudulent or anomalous traffic that needs to be quickly detected to avoid disastrous consequences to the system. Anomalies in sensor traffic may be arise from events internal to the system such as sensor failures or emergency scenarios (such as fire in a building), which are usually benign with nonmalicious intent. Or they may arise from malicious external actors involving dedicated efforts to cause significant damage to the system. A common example of such attack is the distributed denial-of-service attack.

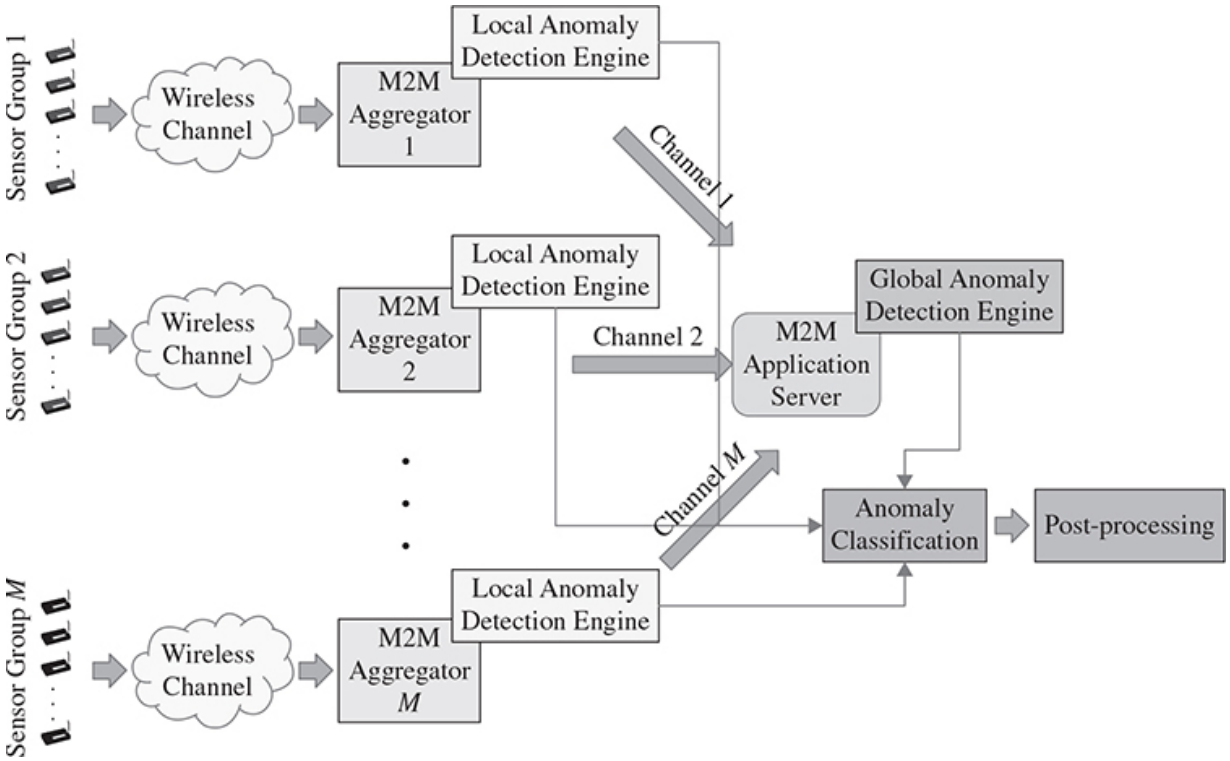


FIGURE 7.1 Anomaly detection framework for M2M system

To detect these anomalies, we propose to implement a local anomaly detection engine at each MA. It stores the specific procedures for detecting each kind of anomaly. The anomaly detection at MAs are basically volumetric and/or feature-based detection methods. Volumetric techniques depend on the number of packets arriving at MAs and in general have low implementation complexity. However, they are not good at detecting sophisticated attacks that are not accompanied with appreciable change in traffic volume. Additionally, they suffer from relatively high false-alarm rate for high anomaly detection probabilities. On the contrary, feature-based technique utilizes some measurable traffic characteristics such as entropy of source or destination address. They can detect a very wide spectrum of anomalies but suffer from high complexity.

It is important to point out here that there may be anomalies that cannot be detected by either volumetric or feature-based detection methods at individual MA. This may occur due to minuscule changes in traffic volume at each MA or the target feature for detecting the anomaly requires analysis of the traffic across MAs. For detecting these sophisticated attacks, we propose to implement a global anomaly detection engine at the M2M AS.

Again, the global anomaly detection engine can be volumetric and/or feature-based depending on the particular anomaly.

The anomalies detected at MAs or AS are forwarded to an anomaly classification engine that contains rules for classifying anomalies that generate similar signature at the anomaly detection engine. Lastly, the detected and classified anomalies along with their metadata are passed to the postprocessing step to take appropriate defensive action to protect the system.

7.3 Anomaly Detection Metrics

We now propose a set of volumetric and feature-based anomaly detection metrics used in this work. For this, we first divide the time horizon into time-slots, each of duration T sec. Then let k $(\forall\ k\ \in\ \mathbb{Z}^{+})$ denote the discrete time-index mapped to the time-slot $[(k-1)T, kT]$, and let the set $\mathcal{K}$ = (1,2, . . . ,k}.

Volumetric metric: The volumetric metric considered in this chapter is number of packets arrived at ith MA or AS in kth time-slot denoted by $N_i(k)$ and $N(k)$, respectively.

Feature-based metrics: We first define an *M2M connection* between a sensor and its corresponding MA, if the MA receives at least one packet from that particular sensor. The first metric we consider, involves building up a database of unique M2M connections made at each MA during a training period, $t \in [0, k_o T]$. Mathematically, we have,

$$H_i(k) = \cup_{m \in \mathcal{K}}\, h_i(m)\ \forall\, k \leq k_o \tag{7.1}$$

where $H_i(k)$ are the contents of the database at ith MA at the end of kth time-slot and $h_i(m)$ is the list of M2M connections made during mth time-slot at ith MA.

After the training period, the database at each MA is used to search for anomalies in each time-slot by determining the number of new M2M connections that are not present in the database. Mathematically, we have,

$$C_i(k) = h_i(k) \setminus H_i(k_o) \; \forall \, k > k_o \tag{7.2}$$

where $C_i(k)$ denotes the number of new M2M connections at ith MA during the *k*th time-slot.

Another feature-based metric we consider in this work is the total number of M2M connections made at ith MA over a sliding window of k_a time-slots. So at the *k*th time-slot we have,
$A_i(k) = |\cup_{m \in \mathcal{K}_a} h_i(m)| \; \forall \, k \geq k_a$. Here the set
$\mathcal{K}_a = \{k - k_a + 1, k - k_a + 2, \cdots, k\}$ and the set operator |. | denotes the cardinality of the set.

7.4 Anomaly Detection and Classification

In this section, we detect the anomalies using the volumetric or/and feature-based metrics and attribute them to either a DDoS attack, an emergency scenario, or device failures.

7.4.1 Distributed Denial-of-Service Attack or Emergency Scenario

The DDoS attack in an M2M application employs a botnet comprising sensors that have been compromised using malicious software to send spam messages to the MAs. This leads to depletion of communication and computational resources at MAs and AS, and thus prevents the legitimate sensors from communicating to MAs. DDoS attacks are marked by increase in traffic volume. However, due to the distributed nature of attack, the increase in traffic at individual MAs may not be significant. Another reason for this is to evade detection at the MAs. Therefore, the global volumetric metric at AS, *N(k)*, may be more useful in this case. Alternatively, the DDoS attacks can be detected by searching for new M2M connections made during the attack, as measured by the metric *Ci(k)* for *i*th MA.

To safeguard an M2M system in the event of a disastrous situation (such as fire in a building), a set of sensors actively transmit alarm messages to the MA when they sense the calamity, that is, the measured physical quantity exceeds a predefined threshold. This again is marked by significant increase in the traffic volume at MAs that lie in the disaster zone and thus can be detected using the local volumetric metric *Ni(k)* at the *i*th MA.

Alternatively, the emergency can be detected by searching for new M2M connections made by the emergency sensors, as measured by the metric *Ci(k)* for *i*th MA.

We note that both DDoS and emergency scenario result in similar signatures for the feature-based detection metric *Ci(k).* However, it is important to distinguish between the two anomalies as they warrant a different set of responses from the system operators. To differentiate between the two cases, we compute an MCD metric for the anomalous packet streams using the following procedure,

1. Select any two anomalous packet streams, *P* and Q, arriving at a given MA.
2. Select subset of arrival epochs *P* and *Q* by defining $p = P[r : r + n_c]$ and $q = Q[1 : n_c]$. Here *r* is the offset between *P* and *Q* and n_c is the number of arrivals used for computation.
3. Synchronize the start of streams $p = p - (p[1] - q[1])$, if $p[1] > q[1]$ or $q = q - (q[1] - p[1])$, if $p[1] < q[1]$.
4. Compute the MCD as

$$d(p,q) = \sum_{j=1}^{n} \frac{|p[j] - q[j]|}{|p[j]| + |q[j]|} \tag{7.3}$$

Since the emergency detecting sensors have similar packet interarrival time epochs, we expect the MCD for packet streams from any two sensors to be 0. On the contrary, the packet arrivals from DDoS compromised sensors are usually independent of each other. This is done to obfuscate the anomaly detection engine that is searching for any patterns in traffic characteristics to detect anomalies.

7.4.2 Device Failures

The terminal devices or sensors in an M2M application might malfunction due to hardware/software problems or be down due to battery exhaustion. It is important to detect and repair these devices as soon as possible;

otherwise it may lead to a system failure. The local volumetric metric N(k) proposed earlier can be used to detect these anomalies by searching for dip in traffic volume at the *i*th MA. Alternatively, we can use the feature-based detection metric $A_z(k)$ at time-slot k by searching for dip in total number of M2M connections at the z'th MA over the time duration of k_a previous time-slots. Now under normal system operation, the total number of connections in a sufficiently large window $\mathcal{K}_a$ is equal to the number of devices registered at the MA. Therefore, the reduction in connections can be used to infer the number of devices that are not functioning.

7.5 Numerical Results

In this section, we use Monte Carlo simulations to evaluate the performance of proposed anomaly detection and classification framework. The time horizon for the simulation is set to 20 sec. The number of MAs is set to 20 and number of sensors per MA is 100. Since different sensors have potentially different packet arrival rates, we assume it to be uniformly distributed between 1 and 3 packets/sec. The number of sensors for detecting emergencies is set to 5 per MA. Lastly, the duration of each time-slot is $T = 1$ sec.

7.5.1 Distributed Denial-of-Service Attack

We consider a botnet comprising of 32 compromised devices uniformly distributed across the M2M network. The attacker increases the packet arrival rate for each compromised sensor negligibly by 0.0032 packet/sec. For simplicity of exposition, we assume the attack lasts from 10 sec to 11 sec. Figure 7.2 shows that the local volumetric detection at an MA fails to detect the attack due to relatively low attack volume. However, on analyzing the aggregated traffic volume at M2M AS, the attack may be detected as shown in Figure 7.3. But it can also generate several false alarms if the detection threshold (i.e., target packet volume) is low.

To overcome this limitation and get clean anomaly detection, we resort to the feature-based detection approach as shown in Figure 7.4. We first create a database for known M2M connections at any MA (say MA 2) until $ko = 4$ timeslots and then use it to detect anomalies by determining any new M2M connections. If the training period is too small, we have a noise floor

due to the legitimate M2M connections that were not identified in the training phase. On the other hand, we can set the training period quite large to detect all legitimate M2M connections. But it leads to higher resource consumption at MAs and also has an opportunity cost in terms of time missing out on anomalies during that training phase.

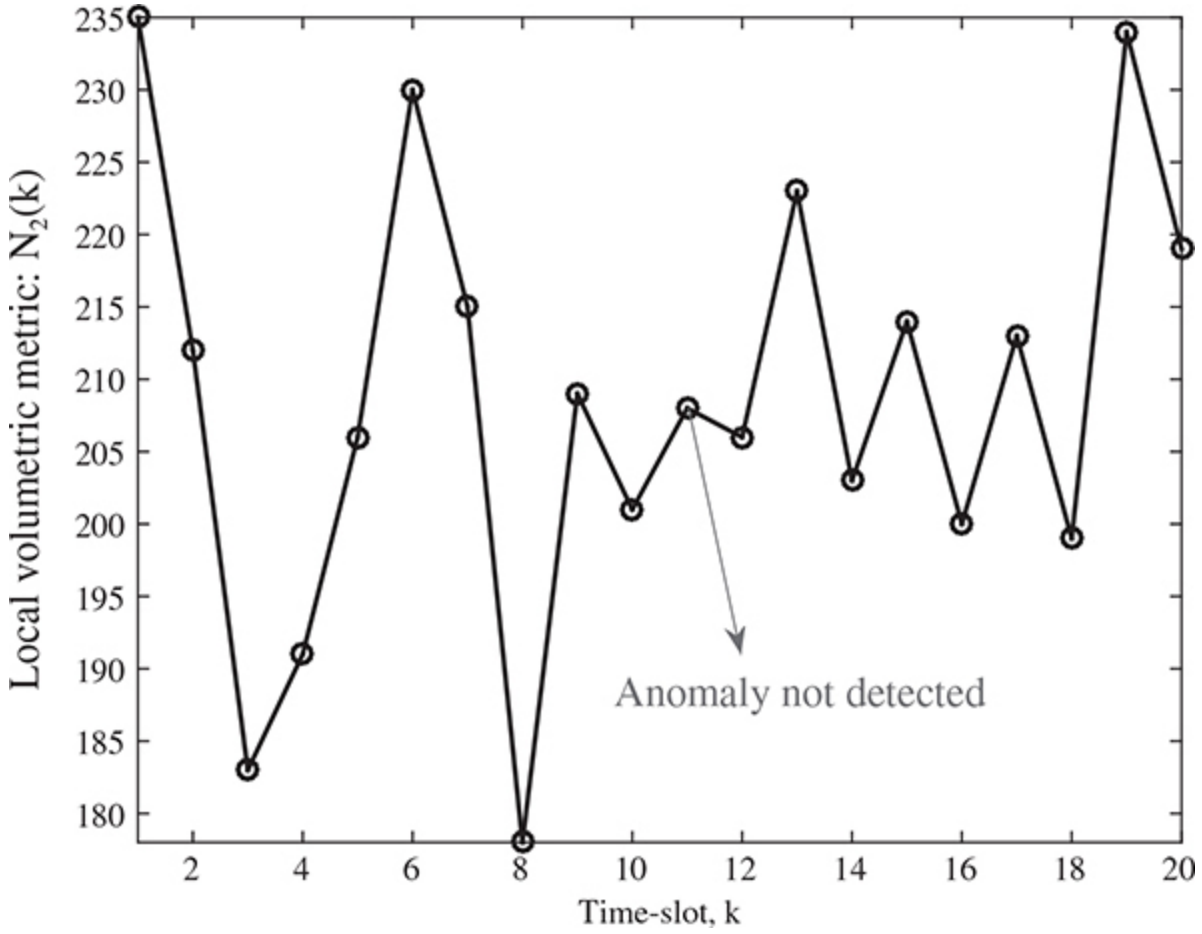


FIGURE 7.2 Local volumetric detection for DDoS attack at MA 2.

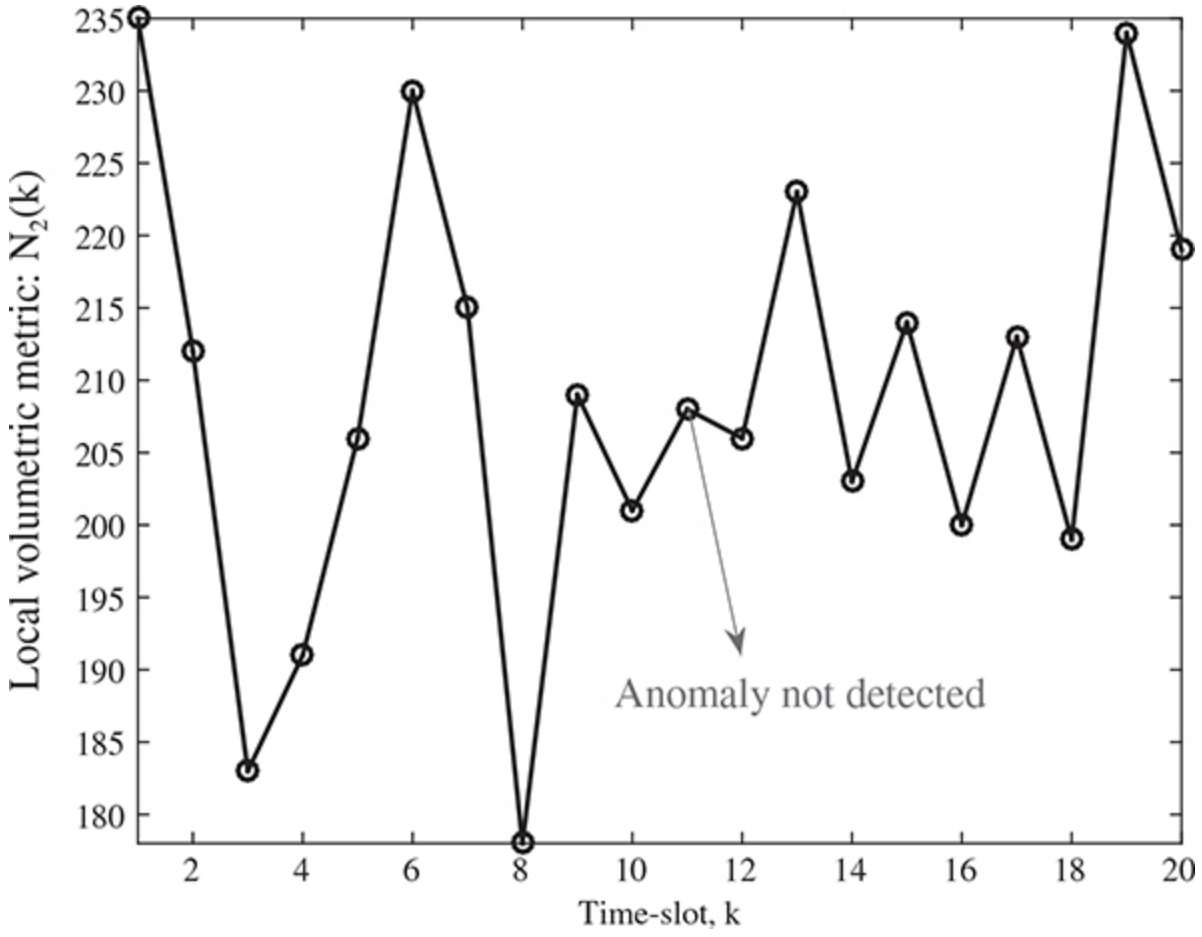


FIGURE 7.3 Global volumetric detection for DDoS attack at M2M AS.

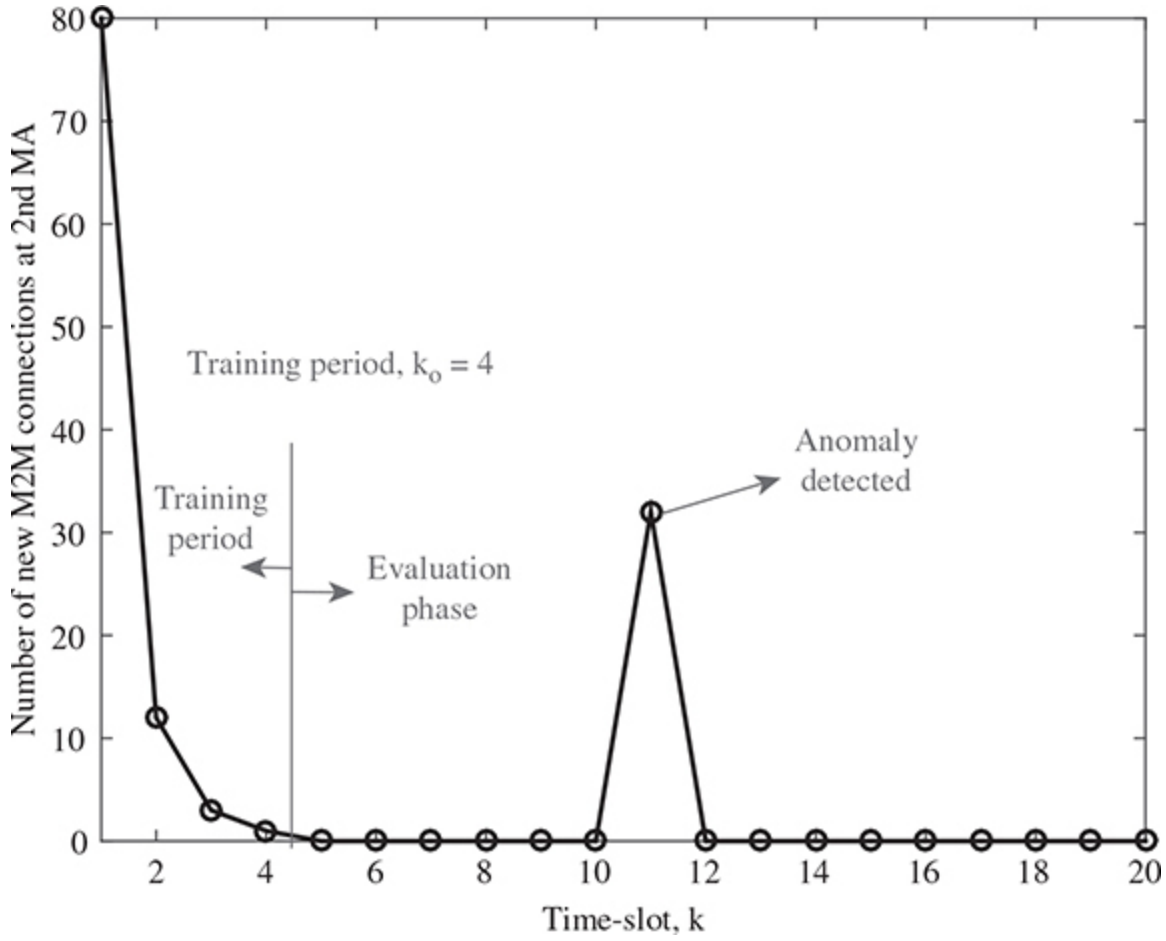


FIGURE 7.4 Feature-based DDoS detection at MA 2.

7.5.2 Emergency Scenario

Assume a disaster situation occurs in the coverage area of MA 2 from 13 sec to 14 sec. On detecting the emergency, the emergency sensors transmit alarm messages to MA 2 at a high rate of 25 packets/sec. The significant increase in traffic volume corresponding to the emergency can be easily detected as shown in Figure 7.5. Furthermore, the feature-based detection method can also be used to detect the emergency, similar to that for DDoS attack. Figure 7.6 illustrates this by plotting the number of new M2M connections during the evaluation phase after the database is trained for k_o = 3 time-slots.

Since the feature-based metric yields the same signature for both DDoS and emergency scenario, we apply the MCD (described in Section 7.4.1) to distinguish between the 2 anomaly classes. Figure 7.7 shows the plot of

MCD applied to any 2 anomalous DDoS or emergency packet streams. As expected, we find that the MCD is 0 for emergency packet streams whereas it is relatively large for DDoS attack. This is true for all values of the packet offset r.

7.5.3 Device Failures

We now consider the detection of device failures. We assume 2 devices in coverage area of MA 2 are malfunctioning and do not transmit to MA 2 from 10 sec to 16 sec. We first use local volumetric analysis to detect device failures at MA 2 as shown in Figure 7.8. We note that it is not tough to detect device failures due to randomness in the number of packets arriving at MAs per time-slot. The problem is worsened when number of failures is small compared to total number of devices. This is true for our simulation as just 2 out of 100 devices are not working.

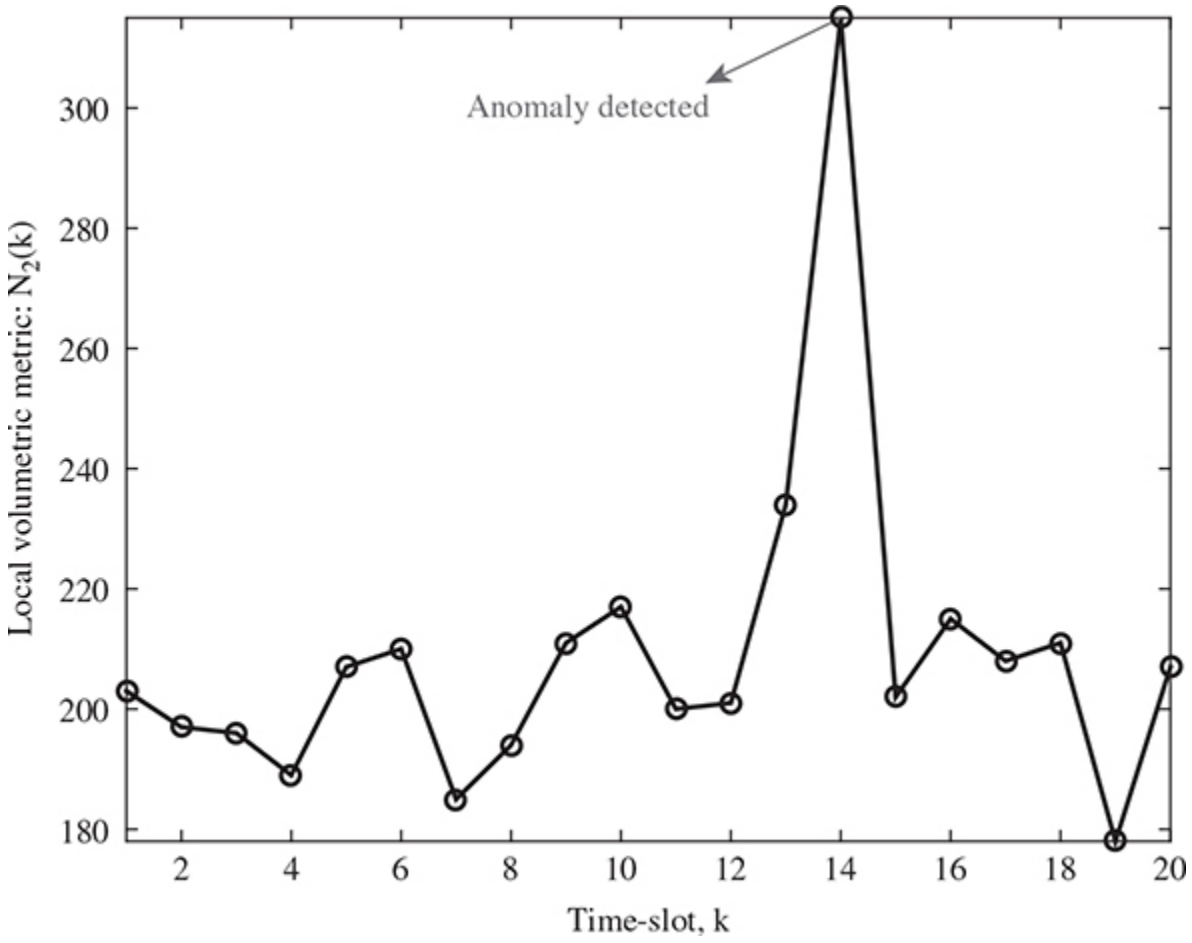


FIGURE 7.5 Local volumetric detection for emergency situation at MA 2.

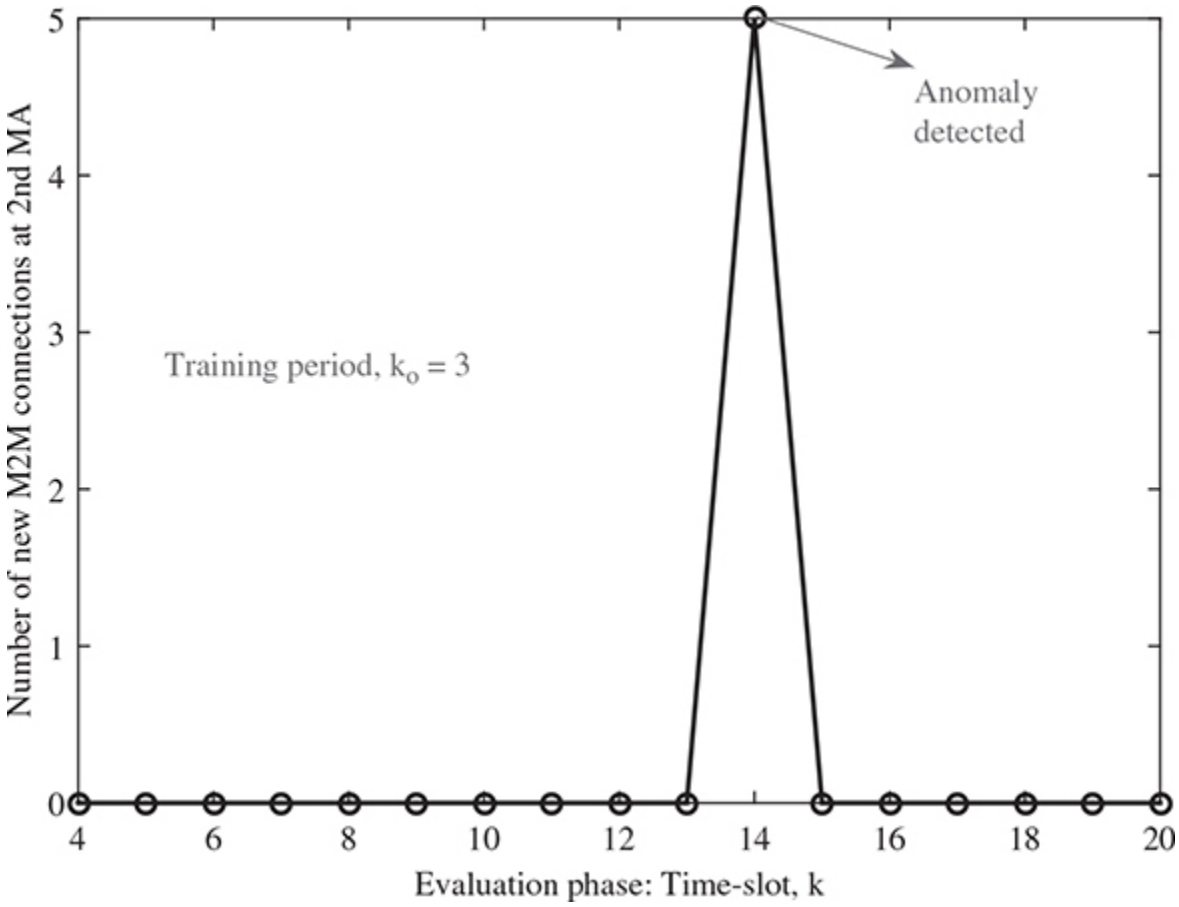


FIGURE 7.6 Feature-based emergency scenario detection at MA 2.

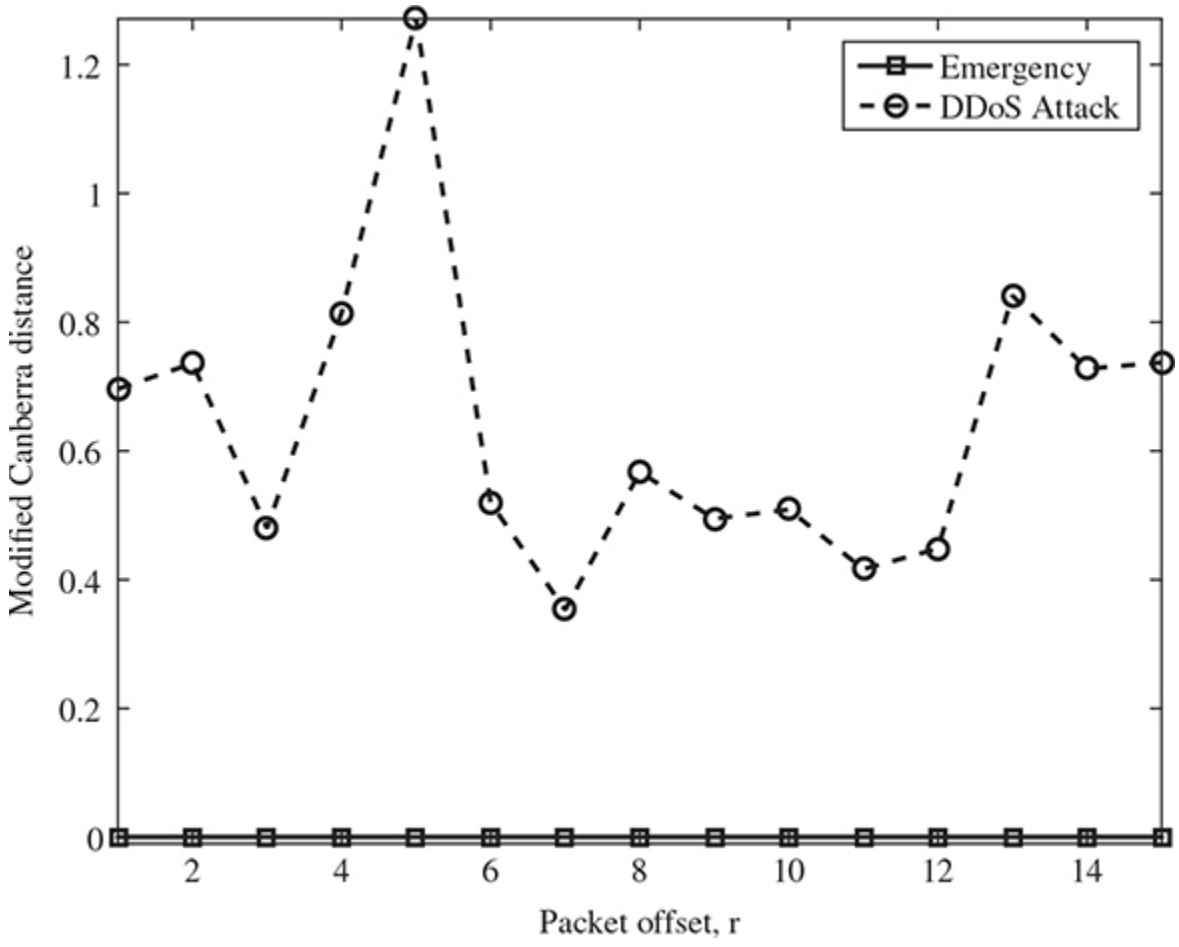


FIGURE 7.7 Modified Canberra metric to distinguish between DDoS attack and emergency scenario. The metric is computed over a window of $n_c = 10$ packets.

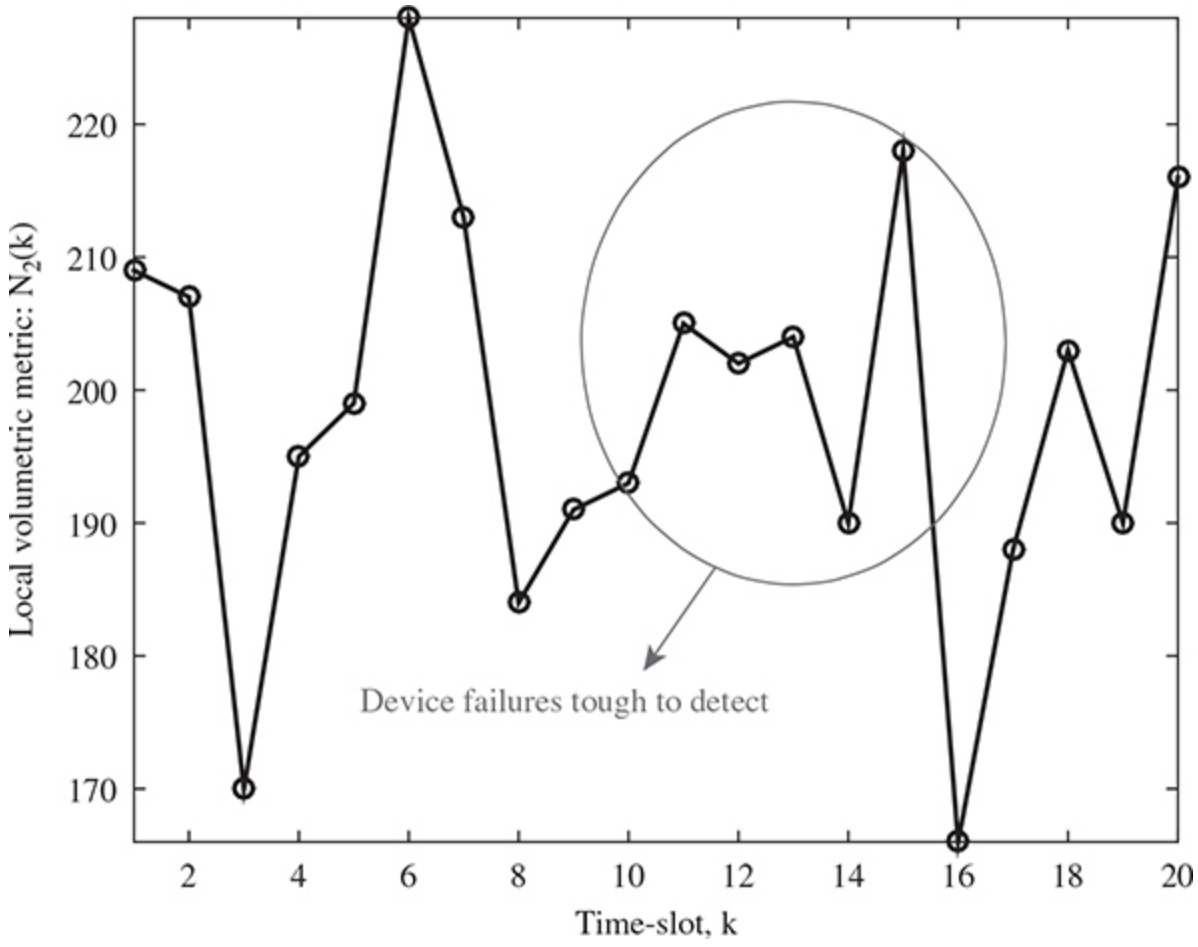


FIGURE 7.8 Local volumetric detection for failure of devices connected to MA 2.

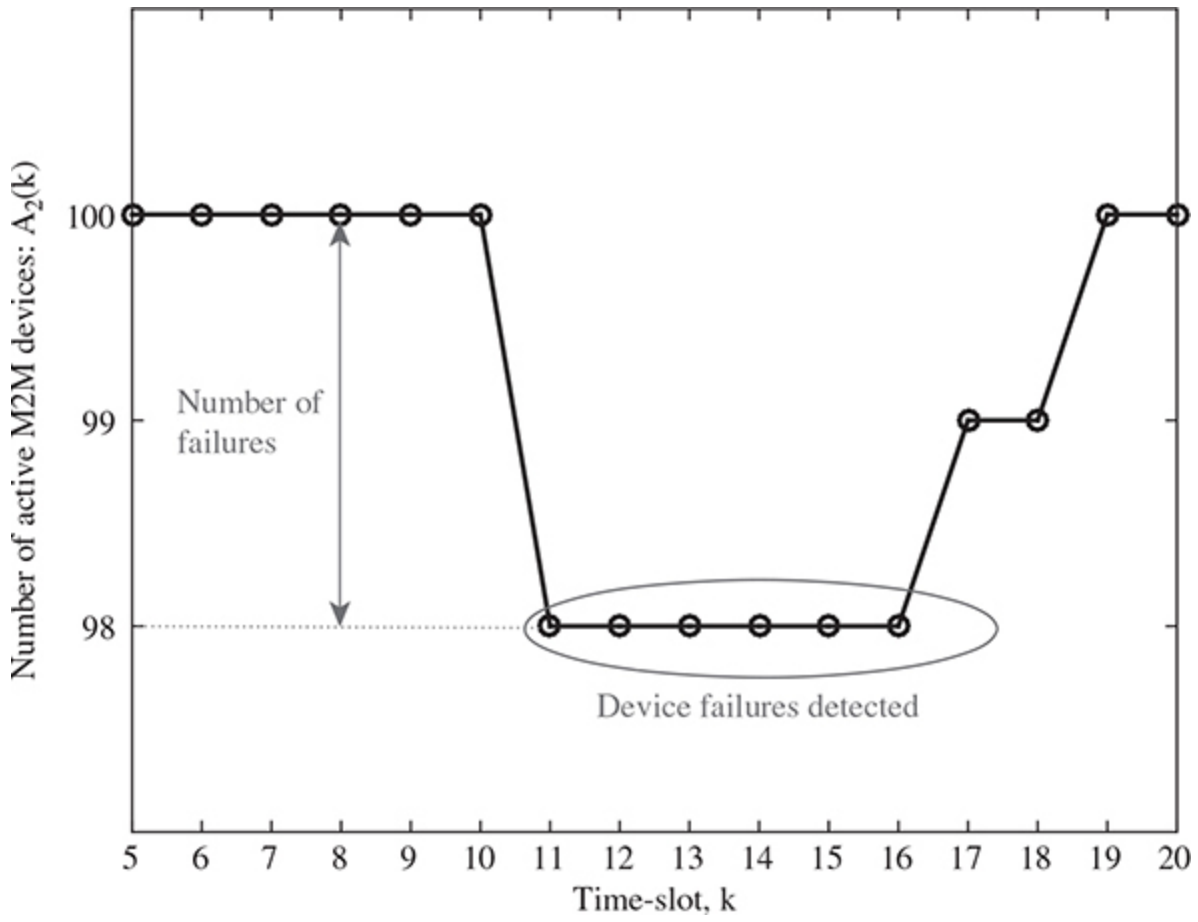


FIGURE 7.9 Feature-based detection of device failures with $k_a = 5$.

In order to improve the detection, especially at low failure rates, we resort to the proposed feature-based technique. Specifically, we compute the total number of M2M connections made over a sliding time-window of k_a time-slots. Figure 7.9 plots the metric $A_2(k)$ as a function of time-slots with $k_a = 5$. The value of k_a is set large enough to ensure at least one packet from each functioning device. We note a clear reduction in number of active devices or M2M connections from 11 sec to 16 sec.

Table 7.1 summarizes the performance of volumetric and feature-based anomaly detection schemes for various anomalies considered in this chapter. For each anomaly type, the feature-based technique always performs better than its volumetric counterpart because it is designed to capture the unique variations in traffic characteristics induced by the anomaly of interest. The global volumetric techniques are not very relevant for detecting emergency scenarios and device failures. This is because these

events manifest primarily as anomalies in the aggregated traffic at the MA to which the anomalous devices are connected. In fact, if global volumetric techniques are used, then it would be harder to detect these anomalies due to the increase in the nonanomalous traffic at the AS, arriving from other MAs.

Anomaly Type	Local Volumetric	Global Volumetric	Feature-Based
DDoS	Poor	Fair	Good
Emergency	Fair	Poor	Good
Device failures	Fair	Poor	Good

TABLE 7.1 Comparative Performance Analysis of Proposed Anomaly Detection Schemes

7.6 Conclusion

In this chapter, we presented novel anomaly detection and classification schemes for M2M uplink. The proposed intrusion detection framework consists of local and global anomaly detection engine at M2M aggregators and M2M application server, respectively. The detected anomalies are then forwarded to an anomaly classification engine and finally sent to the postprocessing operation. To overcome the generally poor detection performance of volumetric anomaly detection techniques, we proposed novel feature-based detection schemes for detecting DDoS attack, emergency scenarios, and device failures. The proposed feature-based schemes are built on predetermining the legitimate M2M connections and then flagging the new M2M connections as anomalies during the evaluation phase. We also proposed an MCD metric to distinguish between the DDoS attack and emergency scenarios, which have similar signatures for proposed volumetric and feature-based detection schemes. It basically measures the similarity or differences in the characteristics of inter-arrival time epochs for any 2 anomalous streams. Device failures are detected by inspecting for the decrease in active M2M connections over a reasonably large time interval. Using extensive Monte Carlo simulations for the M2M uplink system, we showed that the proposed anomaly detection techniques

accurately detect different anomalies with very low false alarms. Future extension of our work to include game theoretical approaches [287-290] can benefit our scheme as in [197].

[1] The content in this chapter is reproduced with permission after modifications (license number 4639361213090). For the original article, refer to [282].

CHAPTER 8

Conclusion and Future Work

Haya Shajaiah and Ahmed Abdelhadi

This book addresses the performance and security of emerging Internet of Things (IoT) wireless technologies. It presented the major performance and security challenges that affect different types of IoT communications. It proposed different mathematical approaches to improve the performance of IoT communications and develop security countermeasurements for different types of IoT security threats.

The performance of IoT communications relies very much on the radio spectrum allocation. Spectrum sharing increases the efficiency of spectrum usage by enabling wireless systems to harvest underutilized swathes of spectrum. A secure spectrum auction **MTSSA** is developed for a multitier dynamic spectrum sharing system. The proposed approach considers spectrum reusability and the case of heterogeneous frequency bands. It leverages Paillier cryptosystem and a federal gateway to keep the base stations' (BSs') bidding values unknown to the auctioneer and find the winning BSs and their charging prices. This prevents possible frauds and bid-rigging between an insincere auctioneer and greedy BSs. Simulation results showed that **MTSSA** achieves an efficient spectrum utilization, revenue, and bidders' satisfaction. A resource allocation with joint carrier aggregation optimization approach is developed. It uses utility proportional fairness approach. The optimization problem is proved to be convex, and therefore the global optimal solution is tractable. A robust distributed resource allocation algorithm is presented to solve the optimization problem and is provided to be providing optimal rates in high-traffic and low-traffic situations. In addition, the book presented an optimal bidding mechanism for determining true bidding values to be used in secure spectrum auctions by BSs that belong to different wireless system providers (WSPs)

participating in a spectrum auction. A resource allocation based on carrier aggregation approach is presented to determine the BS's optimal aggregated rate allocated to each user equipment (UE). Simulation results showed the success in the performance of the proposed optimal bidding strategy.

The proposed spectrum auction mechanisms presented in this book have only considered spectrum heterogeneity in terms of the spectrum being commercial or federal. However, spectrum heterogeneity of the auctioneer's spectrum bands (i.e., spectrum bands with different central frequencies) has not been taken into consideration. Spectrums with different frequencies have different path losses, and therefore different transmission ranges. For example, in a spectrum auction, when considering BSs (bidders) in cellular networks that have macro cells and micro/pico/femto cells, each bidder has different targeted cell coverage when bidding for spectrum bands; that is, macro cells' BSs may favor low-frequency spectrum because of its long transmission range, whereas femto cells' BSs would prefer high-frequency spectrum with transmission range that is enough for an indoor area as it generates less cross-tier interference. In addition, when constructing a conflict graph for bidders participating in a spectrum auction, bidders that are bidding for high-frequency spectrum bands and are considered interference free (i.e., not connected directly to each other in the conflict graph) could cause interference to each other when bidding for low-frequency spectrum bands. Therefore, the conflict graph in a spectrum auction with heterogeneous spectrum bands (have different central frequencies) is not fixed during the auction process. Designing a robust spectrum auction with heterogeneous spectrum bands that achieves high-spectrum utilization while satisfying the essential economic properties, which is required in a successful auction, is a challenging task. Future research work in spectrum auctions needs to address this concern.

Furthermore, smart grid security challenges are discussed and a security and privacy protection method for smart grid communications is proposed. The book presented a secure scheduling mechanism for smart grid power resources through auction process. The scheduling auction mechanism schedules the power plant's limited electric power resources during peak hours time-slots. The proposed power auction leverages homomorphic encryption through Pail-lier cryptosystem to provide a secure and honest auction mechanism by avoiding possible frauds and bid-rigging. Simulation results showed the performance of the proposed power scheduling auction

and its ability to maximize the performance metrics in order to guarantee a successful power auction.

Uplink secrecy in IoT is very essential since the uplink communications contain data of potentially classified sensor reports. An uplink communication of latency-limited industrial IoT networks communicating critical sensor data is considered. We presented an attack resilient system framework for sensor data reporting on the IoT uplink. The proposed approach provided countermeasures to passive attacks from an eavesdropper capable of intercepting transmissions on the uplink and study the cost of security in terms of latency and backhaul rate. Future work in this paradigm will account for additional countermeasures for passive attacks such that secrecy can be achieved at a potentially lower cost. Furthermore, active attacks from IoT classes will be considered where rogue local access points (LAPs) can flood the small cell access point (SAP) with spurious packets thereby crippling the network. The methods developed in this work can be extended to include other networks such as vehicular networks, multicast networks, and other wireless networks.

In addition, cyber-vulnerabilities of the IT system for machine-to-machine (M2M) networks being connected to the Internet at large are considered.We proposed a novel anomaly detection and classification framework for a general M2M uplink system to detect distributed denial-of-service (DDoS) attacks, emergency scenarios, and terminal device failures. A modified Canberra distance metric is proposed to distinguish between DDoS attack and emergency scenarios that yield similar signatures for anomaly detection schemes. The proposed anomaly detection schemes are showed through simulation results to have high-detection performance and low-false alarm rate.

APPENDIX A

MATLAB Code for IoT Spectrum Sharing

```
%1. Main Code
function UE
close all
clear all
clc
syms x
global p_old

%% Utility Parameters
a = [5 3 1];
b = [10 20 30];
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%% START of R LOOP  %%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
for i_rate = 1:19
    % Maximum Rate
    Rate(i_rate) = 10 + i_rate * 10
    % Initial Bids
    w1 = [1 1 1 1 1 1 1 1 1 1 1 1];   % macro cell
       users (7:12) and small cell users (1:6) bidding
       for resources from macro cell eNoeB "Carrier 1"
    w2 = [5 5 5 5 5 5];   % small cell users bidding
       for resources from small cell eNodeB "Carrier 2"
    % Initial Rates
    r21_opt = [0 0 0 0 0 0];
    r22_opt = [0 0 0 0 0 0];
    r1_opt = [0 0 0 0 0 0];
    r_inflection = [b 0 0 0];
```

```
26      r21_min = [0 0 0 0 0 0]; % initial new min_rate of
           optimization Group 2 macro 1
27      r22_min = [0 0 0 0 0 0]; % initial new min_rate of
           optimization Group 2 small 2
28      r1_min = [0 0 0 0 0 0]; % initial new min_rate of
           optimization Group 1 macro 1
29      △1 = 1;
30      △2 = 1;
31      time = 0;
32          while  (△1 > 0.0001) && (△2 > 0.0001) |
               (time<10)%
33          time = time + 1;
34          w1_old = w1;   % macro cell  Carrier 1
35          w2_old = w2;   % small cell  Carrier 2
36          t(time) = time;
37
38          p1(time) = eNodeB1varR(w1,Rate(i_rate));  %
               sent from eNodeB macro cell Carrier1
39          p2(time) = eNodeB2(w2);  % sent from eNodeB
               small cell Carrier2
40
41          %%%%%%%%%%%%%%%%%% Group of users 1
               %%%%%%%%%%%%%%%%%%
42          for ig1 = 1: 2*length(a)
43              pp11 = p1(time);
44              ii1 =ig1;
45              r1 = r1_opt(ii1);
46              soln11(ig1) = fzero(@(x)
                   utility(x,ii1,pp11),[.01 1000]);
47              r1_opt(ig1) = max(soln11(ig1), r1_min(ig1));
48              w1(ig1+6) = r1_opt(ig1) * p1(time);
49              if abs(w1_old(ig1+6)-w1(ig1+6)) > (5.*
                   exp(-0.1*time))%(10 ./ time)
50                  w1(ig1+6) = w1_old(ig1+6) + (5.*
                       exp(-0.1*time)) .*
                       sign(w1(ig1+6)-w1_old(ig1+6));
51              end
52          end
53                  %%%%%%%%%%%%%%%%%% Group of users 2
                       %%%%%%%%%%%%%%%%%%
54          for ig3 = 1: 2*length(a)
```

```
55                pp1 = p1(time);
```

```
56              pp2 = p2(time);
57              ii =ig3;
58              r21 = r21_opt(ii);
59              r22 = r22_opt(ii);
60              %%%%%%%% solve for carrier 1
                   %%%%%%%%%%%%%%%%%%%%%
61                  soln1(ig3) = fzero(@(x)
                       utility(x,ii,pp1),[.01 1000]);
62                  if soln1(ig3) > r22_opt(ig3)
63                      soln1(ig3) = soln1(ig3) -
                           r22_opt(ig3);
64                  else
65                      soln1(ig3) = 0;
66                  end
67                  r21_opt(ig3) = max(soln1(ig3),
                       r21_min(ig3));
68                  w1(ig3) = r21_opt(ig3) * p1(time);
69                                  %%%%%%%% solve for
                                       carrier 2
                                       %%%%%%%%%%%%%%%%%%%%%
70                  soln2(ig3) = fzero(@(x)
                       utility(x,ii,pp2),[.01 1000]);
71                  if soln2(ig3) > r21_opt(ig3)
72                      soln2(ig3) = soln2(ig3) -
                           r21_opt(ig3);
73                  else
74                      soln2(ig3) = 0;
75                  end
76                  r22_opt(ig3) = max(soln2(ig3),
                       r22_min(ig3));
77                  w2(ig3) = r22_opt(ig3) * p2(time);
78
79              if abs(w1_old(ig3)-w1(ig3)) > (5.*
                   exp(-0.1*time))%(10 ./ time)
80                  w1(ig3) = w1_old(ig3) + (5.*
                       exp(-0.1*time)) .*
                       sign(w1(ig3)-w1_old(ig3));
81              end
82              if abs(w2_old(ig3)-w2(ig3)) > (5.*
                   exp(-0.1*time))%(10 ./ time)
83                  w2(ig3) = w2_old(ig3) + (5.*
```

```
exp(-0.1*time)) .*
```

```
                    sign(w2(ig3)-w2_old(ig3));
84              end
85                      end
86          w21_sim(time,:) = w1(1:6);   % bid group 2
               carrier 1
87          r21_sim(time,:) = w21_sim(time,:)./p1(time);
88          △1 = max(abs(w1-w1_old));
89          w22_sim(time,:) = w2(1:6);   % bid group 2
               carrier 2
90          r22_sim(time,:) = w22_sim(time,:)./p2(time);
91          △2 = max(abs(w2-w2_old)) ;
92          w1_sim(time,:) = w1(7:12);   % bid group 1
               carrier 1
93          r1_sim(time,:) = w1_sim(time,:)./p1(time);  %
               rates group 1 carrier 1
94              end   % (while) end of the time iteration
95      r1_ss(i_rate,:) = r1_sim(time,:);
96      r21_ss(i_rate,:) = r21_sim(time,:);
97      r22_ss(i_rate,:) = r22_sim(time,:);
98      w1_ss(i_rate,:) = w1_sim(time,:);
99          w21_ss(i_rate,:) = w21_sim(time,:);
100     w22_ss(i_rate,:) = w22_sim(time,:);
101     p1_ss(i_rate) = p1(time);
102     p2_ss(i_rate) = p2(time);
103     time_ss(i_rate) = time;
104 end
105 p1_ss
106 p2_ss
107 S1 = sum(r1_ss,2).*p1_ss'
108 S2 = sum(r21_ss,2).*p1_ss'
109 S3 = sum(r22_ss,2).*p2_ss'
110 S=S1+S2+S3
111 r1_ss
112 Rates = r1_ss
113 Mul_U_Macro = Utilityy(Rates)
114
115 figure;
116 plot(Rate,r1_ss(:,1),
       '-r.','LineWidth',1.8,'MarkerSize',25)
117 hold on
118 plot(Rate,r1_ss(:,2),
```

```
        '-gs','LineWidth',1.8,'MarkerSize',10)
```

```
hold on
plot(Rate,r1_ss(:,3),
    '-mo','LineWidth',1.8,'MarkerSize',10)
hold on
plot(Rate,r1_ss(:,4),
    '-cd','LineWidth',1.8,'MarkerSize',10)
hold on
plot(Rate,r1_ss(:,5),
    '-b*','LineWidth',1.8,'MarkerSize',10)
hold on
plot(Rate,r1_ss(:,6),
    '-k+','LineWidth',1.8,'MarkerSize',10)
I=legend(' $i = 1$',' $i = 2$',' $i = 3$',' $i = 4$','
    $i = 5$',' $i =
    6$','Interpreter','latex','FontName','Times New
    Roman','fontSize',20,'fontWeight','bold');
axis([30 200 0 50])
xlabel('$R_1$','Interpreter','latex','FontName','Times
    New Roman','fontSize',30,'fontWeight','bold');
ylabel('$r_{1i}$','Interpreter','latex','FontName',
    'Times New Roman','fontSize',30,'fontWeight','bold');
set(gca,'FontName','Times New Roman','FontSize',24)
set(I,'interpreter','latex');
set(I,'FontSize',30);
set(I,'FontWeight','bold');
figureHandle = gcf;
set(findall(figureHandle,'type','text'),'FontName',
    'Times New Roman','fontSize',30,'fontWeight','bold')

%%%%%%%%%%%%%%%%%%%%
%Figure2
figure;
plot(Rate,r21_ss(:,1)+r22_ss(:,1),
    '-r.','LineWidth',1.8,'MarkerSize',25)
hold on
plot(Rate,r21_ss(:,2)+r22_ss(:,2),
    '-gs','LineWidth',1.8,'MarkerSize',10)
hold on
plot(Rate,r21_ss(:,3)+r22_ss(:,3),
    '-mo','LineWidth',1.8,'MarkerSize',10)
hold on
```

```
plot(Rate,r21_ss(:,4)+r22_ss(:,4),
    '-cd','LineWidth',1.8,'MarkerSize',10)
hold on
plot(Rate,r21_ss(:,5)+r22_ss(:,5),
    '-b*','LineWidth',1.8,'MarkerSize',10)
hold on
plot(Rate,r21_ss(:,6)+r22_ss(:,6),
    '-k+','LineWidth',1.8,'MarkerSize',10)
I=legend(' $i = 7$',' $i = 8$',' $i = 9$',' $i = 10$','
    $i = 11$',' $i =
    12$','Interpreter','latex','FontName','Times New
    Roman','fontSize',20,'fontWeight','bold');
axis([30 200 0 50])
xlabel('$R_1$','Interpreter','latex','FontName','Times
    New Roman','fontSize',30,'fontWeight','bold');
ylabel('$r_{1i}$+$r_{2i}$','Interpreter','latex',
    'FontName','Times New
    Roman','fontSize',30,'fontWeight','bold');
set(gca,'FontName','Times New Roman','FontSize',24)
set(I,'interpreter','latex');
set(I,'FontSize',30);
set(I,'FontWeight','bold');
figureHandle = gcf;
set(findall(figureHandle,'type','text'),'FontName',
    'Times New Roman','fontSize',30,'fontWeight','bold')
%%%%%%%%%%%%%%%%%%%%
%Figure3
figure;
plot(Rate,r21_ss(:,1),
    '-r.','LineWidth',1.8,'MarkerSize',25)
hold on
plot(Rate,r21_ss(:,2),
    '-gs','LineWidth',1.8,'MarkerSize',10)
hold on
plot(Rate,r21_ss(:,3),
    '-mo','LineWidth',1.8,'MarkerSize',10)
hold on
plot(Rate,r21_ss(:,4),
    '-cd','LineWidth',1.8,'MarkerSize',10)
hold on
plot(Rate,r21_ss(:,5),
```

```
        '-b*','LineWidth',1.8,'MarkerSize',10)
```

```
hold on
plot(Rate,r21_ss(:,6),
    '-k+','LineWidth',1.8,'MarkerSize',10)
I=legend(' $i = 7$',' $i = 8$',' $i = 9$',' $i = 10$','
    $i = 11$',' $i =
    12$','Interpreter','latex','FontName','Times New
    Roman','fontSize',20,'fontWeight','bold');
axis([30 200 0 50])
xlabel('$R_1$','Interpreter','latex','FontName','Times
    New Roman','fontSize',30,'fontWeight','bold');
ylabel('$r_{1i}$','Interpreter','latex','FontName',
    'Times New Roman','fontSize',30,'fontWeight','bold');
set(gca,'FontName','Times New Roman','FontSize',24)
set(I,'interpreter','latex');
set(I,'FontSize',30);
set(I,'FontWeight','bold');
figureHandle = gcf;
set(findall(figureHandle,'type','text'),'FontName',
    'Times New Roman','fontSize',30,'fontWeight','bold')
%%%%%%%%%%%%%%%%%%%%
%Figure4
figure;
plot(Rate,r22_ss(:,1),
    '-r.','LineWidth',1.8,'MarkerSize',25)
hold on
plot(Rate,r22_ss(:,2),
    '-gs','LineWidth',1.8,'MarkerSize',10)
hold on
plot(Rate,r22_ss(:,3),
    '-mo','LineWidth',1.8,'MarkerSize',10)
hold on
plot(Rate,r22_ss(:,4),
    '-cd','LineWidth',1.8,'MarkerSize',10)
hold on
plot(Rate,r22_ss(:,5),
    '-b*','LineWidth',1.8,'MarkerSize',10)
hold on
plot(Rate,r22_ss(:,6),
    '-k+','LineWidth',1.8,'MarkerSize',10)
I=legend(' $i = 7$',' $i = 8$',' $i = 9$',' $i = 10$','
    $i = 11$',' $i =
```

```
12$','Interpreter','latex','FontName','Times New
```

```
    Roman','fontSize',20,'fontWeight','bold');
axis([30 200 0 50])
xlabel('$R_1$','Interpreter','latex','FontName','Times
    New Roman','fontSize',30,'fontWeight','bold');
ylabel('$r_{2i}$','Interpreter','latex','FontName',
    'Times New Roman','fontSize',30,'fontWeight','bold');
set(gca,'FontName','Times New Roman','FontSize',24)
set(I,'interpreter','latex');
set(I,'FontSize',30);
set(I,'FontWeight','bold');
figureHandle = gcf;
set(findall(figureHandle,'type','text'),'FontName',
    'Times New Roman','fontSize',30,'fontWeight','bold')
%%%%%%%%%%%%%%%%%%%%

%%%%%%%%%%%%%%%%%%%%
figure;
subplot(2,1,1)
plot(Rate,r1_ss)
h = legend('$G1 U1 i = 1$','$G1 U2 i = 2$','$G1 U3 i =
    3$','$G1 U4 i = 4$','$G1 U5 i = 5$','$G1 U6 i =
    6$',6);
axis([20 300 0 40])
xlabel('$R_1$')
ylabel('$r_{1i}$')
subplot(2,1,2)
plot(Rate,r21_ss + r22_ss)
h = legend('$G3 U1 i = 13$','$G3 U2 i = 14$','$G3 U3 i
    = 15$','$G3 U4 i = 16$','$G3 U5 i = 17$','$G3 U6 i =
    18$',6);
axis([20 300 0 40])
xlabel('$R_1$')
ylabel('$r_{1i} + r_{2i}$')

figure;
subplot(2,1,1)
plot(Rate,r21_ss)
h = legend('$G3 U1 i = 13$','$G3 U2 i = 14$','$G3 U3 i
    = 15$','$G3 U4 i = 16$','$G3 U5 i = 17$','$G3 U6 i =
    18$',6);
axis([20 300 0 40])
```

```
232 xlabel('$R_1$')
```

```
ylabel('$r_{1i}$')
subplot(2,1,2)
plot(Rate,r22_ss)
h = legend('$G3 U1 i = 13$','$G3 U2 i = 14$','$G3 U3 i
    = 15$','$G3 U4 i = 16$','$G3 U5 i = 17$','$G3 U6 i =
    18$',6);
axis([20 300 0 30])
xlabel('$R_1$')
ylabel('$r_{2i}$')
figure;
P1 = [2.48601 1.00105 0.998987 0.678205 0.0733882
    0.0471757 0.0343537 0.0269051 0.0219997 0.0187281
    0.0157139 0.0141804 0.0131369 0.0117321 0.00998086
    0.0093758 0.00870864 0.00822342];
     length(P1)
n1 = [30 40 50 60 70 80 90 100 110 120 130 140 150 160
    170 180 190 200];
semilogy(n1,P1, '-ro','LineWidth',2,'MarkerSize',10,
    'MarkerFaceColor','r')

hold on
P2 = [0.0730367 0.0730367 0.0730367 0.0730367 0.0730367
    0.0730367 0.0730367 0.0730367 0.0730367 0.0730367
    0.0730367 0.0730367 0.0730367 0.0730367 0.0730367
    0.0730367 0.0730367 0.0730367 0.0730367 0.0730367];
     length(P2)
n2 = [30 40 50 60 70 80 90 100 110 120 130 140 150 160
    170 180 190 200];
semilogy(n2,P2, '-bd','LineWidth',2,'MarkerSize',10,
    'MarkerFaceColor','b')
hold on
semilogy(Rate,p1_ss,'-ro','LineWidth',2,'MarkerSize',13)
hold on
semilogy(Rate,p2_ss,
    '-bd','LineWidth',2,'MarkerSize',10)
y = logspace(-3,-1);
xlim([30 200]);
xlabel('$R_{1}$','Interpreter','latex','FontName','Times
    New Roman','fontSize',30,'fontWeight','bold');
I=legend('$p_{1}$ (multiple-stage RA)','$p_{2}$
    (multiple-stage RA)','$p_{1}$ (Joint CA)','$p_{2}$
```

```
(Joint CA)','Interpreter','latex','FontName','Times
```

```
    New Roman','fontSize',30,'fontWeight','bold');
set(gca,'FontName','Times New Roman','FontSize',24)
set(I,'interpreter','latex');
set(I,'FontSize',30);
set(I,'FontWeight','bold');
figureHandle = gcf;
set(findall(figureHandle,'type','text'),'FontName',
    'Times New Roman','fontSize',30,'fontWeight','bold')
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%Figure6
 figure;
 P1 = [79.6929 45.1546 55.0619 45.8048 10.2497 8.88662
    8.2044 7.80308 7.53253 7.35994 7.15538 7.09783
    7.08311 6.9897 6.80931 6.80021 6.76721 6.75725];
     length(P1)
 n1 = [30 40 50 60 70 80 90 100 110 120 130 140 150 160
    170 180 190 200];


plot(n1,P1, '-go','LineWidth',2,'MarkerSize',10,
    'MarkerFaceColor','g')

 hold on

plot(Rate,S','-ro','LineWidth',2,'MarkerSize',13)

xlim([30 200]);
xlabel('$R_{1}$','Interpreter','latex','FontName','Times
    New Roman','fontSize',30,'fontWeight','bold');
set(gca,'FontName','Times New Roman','FontSize',24)
set(I,'interpreter','latex');
set(I,'FontSize',30);
set(I,'FontWeight','bold');
figureHandle = gcf;
set(findall(figureHandle,'type','text'),'FontName',
    'Times New Roman','fontSize',30,'fontWeight','bold')
% %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

figure;
semilogy(Rate,p1_ss,Rate,p2_ss)
h = legend('$p1$ (Joint CA)','$p2$ (Joint CA)',2);
```

```
292 xlabel('$R_1$')
```

```
293
294 %2. Called by Main
295 function [p1] = eNodeBvarR(w1,R1)
296 p1 = sum(w1)/R1;
297
298 %3. Called by Main
299 function [p2] = eNodeB(w2)
300 global p_old R2
301 R2 = 70;
302 p2 = sum(w2)/R2;
```

APPENDIX B

MATLAB Code for IoT Smart Grid

```
%1. Main Code
clear all;
close all;
clc;
%%% 4 Smart Meters
SM_Num = 6;

for MC = 1:1000
    for EPU_Num = 1:15
        N = EPU_Num;
    Bid_EPU=zeros(N,SM_Num);
    Alloc_4SM = colex(N, SM_Num, 0, N);
        Bid_Alloc_4SM = zeros(size(Alloc_4SM,1),SM_Num);
    for j = 1:SM_Num
        for i = 1:N  %loop for number of EPUs
        if i == 1
        Bid_EPU(i,j) = ( 10.*rand(1,1)); %generate a
           single number in the interval [0,10]
        else
        Bid_EPU(i,j) = Bid_EPU(i-1,j).*( 1.*rand(1,1));
                end
        end
        for l = 1:size(Alloc_4SM,1)
            K = Alloc_4SM(l,j);
            if K== 0
                Bid_Alloc_4SM(l,j);
            else
        Bid_Alloc_4SM(l,j) = sum(Bid_EPU(1:K,j),1);
        end
```

```
                end
    end

    Bid_Alloc_4SM; %This metric in each column is the
       biddings of one SM for all allocations
    %Find the best allocation with all SMs participating
    sum_bids = sum(Bid_Alloc_4SM,2);  %sum each row in
       the bidding matric
    [M1, I1] = max(sum_bids); %find the allocation with
       the max summation of bids
    %For each SM find its payment and utility
    for j = 1 : SM_Num
      sum_bids_without_j = zeros(size(Alloc_4SM,1),1);
      M2=0;
      I2=0;
      sum_bids_without_j =
         sum(Bid_Alloc_4SM,2)-Bid_Alloc_4SM(:,j) ;
      [M2,I2] = max(sum_bids_without_j);
     sum(Bid_Alloc_4SM(I2,1:SM_Num));
      Bid_Alloc_4SM(I2,j);
      Payment_j(j)=(sum(Bid_Alloc_4SM(I2,1:SM_Num),2)
         -Bid_Alloc_4SM(I2,j))-(sum(Bid_Alloc_4SM(I1,
         1:SM_Num),2)-Bid_Alloc_4SM(I1,j));
      utility_j(j)= Bid_Alloc_4SM(I1,j) - Payment_j(j);
    end
        Revenue(EPU_Num) = sum(Payment_j,2);
    Bidder_Satis(EPU_Num) =
       sum(utility_j,2)/sum(Bid_Alloc_4SM(I1,
       1:SM_Num),2);
    end
    Revenue_MC(:, MC) = Revenue(:);
    Bidder_Satis_MC(:, MC) = Bidder_Satis(:);
end
Revenue_T = mean(Revenue_MC,2)
Bidder_Satis_T = mean(Bidder_Satis_MC,2)
Revenue_T_Final = Revenue_T.'
Bidder_Satis_T_Final = Bidder_Satis_T.'
EPU_Num_set=[1:EPU_Num];
figure;
plot(EPU_Num_set,Revenue_T);
xlim([1 EPU_Num])
```

```
62 figure;
```

```
plot(EPU_Num_set,Bidder_Satis_T);
xlim([1 EPU_Num])
ylim([0 1])

%2. Called by Main
function X=colex(n,k,a,b)
% Generate all integer compositions of n with k parts, each between 0 and b
%
% n: integer whose compositions are to be generated
% k: number of parts
% a: minimum value of parts
% b: maximum value of parts
%
% The algorithm is directly taken from
% Vincent Vajnovszki, Generating permutations with a given major index, http://arxiv.org/abs/1302.6558
%
% Matlab implementation:
% Steffen Eger, steffen.eger@yahoo.com, 11/5/2013
%
%

X=[];
if k*a>n || k*b<n || n<0 || k<0
  return
end
[minimum,im] = generateMin(n-k*a,k,b-a);
c = zeros(k,1);
% not impossible
if im==0
    % first, compute all compositions with parts p such that 0≤p≤b-a
    X=genColex(n-k*a,k,k,b-a,c,minimum,[]);
    % then add a such that a≤p≤b
    X = X+a;
end
end

% b is the upper bound
function X=genColex(n,r,k,b,c,minimum,X)
```

```
101 if n==0
```

```
    % leave this if you just want to have it printed out
       (might be memory-saving)
    % disp(c')
    % leave this if want to store results in matrix X
    X(end+1,:)=c;
  else
    if c(r)==b
      r = r-1;
    end
    l = minimum(n);
    for i=l:r
      if i==l
      e = n-(l-1)*b;
      else
      e = 1;
      end
      c(i) = c(i)+e;
      X=genColex(n-e,i,k,b,c,minimum,X);
      c(i) = c(i)-e;
    end
  end
  end

  function [m,impossible]=generateMin(n,k,b)
  m=zeros(n,1);
  impossible=0;
  for i=1:n
     q = find(i,k,b);
     if q==-1
      impossible=1;
      break
     end
     m(i) = q;
  end
  end

  function t=find(n,k,b)
  t=-1;
  for s=1:k
    if s*b≥n
      t=s;
```

```
142       break;

143     end
144   end
145   end
```

References

[1] Q. F. Hassan, *A Tutorial Introduction to IoT Design and Prototyping with Examples,* pp. 153-190. IEEE, 2018.

[2] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for IoT big data and streaming analytics: A survey," *IEEE Communications Surveys & Tutorials,* vol. 20, pp. 2923-2960, Fourth Quarter 2018.

[3] N. Nikaein, M. Laner, K. Zhou, P. Svoboda, D. Drajic, M. Popovic, and S. Krco, "Simple traffic modeling framework for machine type communication," in *IEEE ISWCS*, pp. 1-5, August 2013.

[4] J. Zheng, D. Simplot-Ryl, C. Bisdikian, and H. T. Mouftah, "The internet of things," *IEEE Communications Magazine,* vol. 49, pp. 30-31, November 2011.

[5] S. Vural, P. Navaratnam, N. Wang, C. Wang, L. Dong, and R. Tafazolli, "In-network caching of internet-of-things data," in *IEEE International Conference on Communications (ICC),* pp. 3185-3190, June 2014.

[6] F. Al-Turjman, E. Ever, and H. Zahmatkesh, "Small cells in the forthcoming 5G/IoT: Traffic modelling and deployment overview," *IEEE Communications Surveys & Tutorials,* vol. 21, pp. 28-65, First Quarter 2019.

[7] S. Pattar, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik, "Searching for the IoT resources: Fundamentals, requirements, comprehensive review, and future directions," *IEEE Communications Surveys & Tutorials,* vol. 20, pp. 2101-2132, Third Quarter 2018.

[8] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Communications Surveys & Tutorials,* vol. 21, pp. 2702-2733, Third Quarter 2019.

[9] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the internet of things," *IEEE Communications*

Surveys & Tutorials, vol. 21, pp. 1636-1675, Second Quarter 2019.

[10] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet of Things Journal,* vol. 6, pp. 8182-8201, October 2019.

[11] M. Yi, X. Xu, and L. Xu, "An intelligent communication warning vulnerability detection algorithm based on IoT technology," *IEEE Access,* vol. 7, pp. 164803-164814, 2019.

[12] M. Ghorbonzadeh, A. Abdelhadi, and T. C. Clancy, *Cellular Communications Systems in Congested Environments: Resource Allocation and End-to-End Quality of Service Solutions with MATLAB.* Springer International Publishing, 2017.

[13] A. Khawar, A. Abdelhadi, and T. C. Clancy, "On the impact of time-varying interference-channel on the spatial approach of spectrum sharing between s-band radar and communication system," in *Military Communications Conference (MILCOM)*, 2014.

[14] A. Khawar, A. Abdel-Hadi, and T. C. Clancy, "Spectrum sharing between s-band radar and LTE cellular system: A spatial approach," in *2014 IEEE International Symposium on Dynamic Spectrum Access Networks: SSPARC Workshop (IEEE DySPAN 2014 - SSPARC Workshop)* (McLean, USA), April 2014.

[15] H. Shajaiah, A. Khawar, A. Abdel-Hadi, and T. Clancy, "Resource allocation with carrier aggregation in LTE advanced cellular system sharing spectrum with s-band radar," in *Dynamic Spectrum Access Networks (DYSPAN), 2014 IEEE International Symposium*, pp. 34-37, April 2014.

[16] M. Ghorbanzadeh, A. Abdelhadi, and C. Clancy, "Quality of service in communication systems," in *Cellular Communications Systems in Congested Environments,* pp. 1-20, Springer, 2017.

[17] Federal Communications Commission (FCC), "Connecting America: The national broadband plan." Online, 2010.

[18] Federal Communications Commission, "Proposal to Create a Citizen's Broadband Service in the 3550-3650 MHz band," 2012.

[19] A. Khawar, A. Abdel-Hadi, T. Clancy, and R. McGwier, "Beampattern analysis for mimo radar and telecommunication system coexistence," in *Computing, Networking and Communications*

(ICNC), 2014 International Conference on, pp. 534-539, February 2014.

[20] B. Bahrak, S. Bhattarai, A. Ullah, J.-M. Park, J. Reed, and D. Gurney, "Protecting the primary users' operational privacy in spectrum sharing," in *Dynamic Spectrum Access Networks (DYSPAN), 2014 IEEE International Symposium on*, 2014. [21] A. Khawar, A. Abdelhadi, and T. C. Clancy, "QPSK waveform for MIMO radar with spectrum sharing constraints," *CoRR*, vol. abs/1407.8510, 2014.

[22] L. S. Wang, J. P. McGeehan, C. Williams, and A. Doufexi, "Application of cooperative sensing in radar-communications coexistence," *IET Communications*, vol. 2, pp. 856-868, 2008.

[23] J. A. Mahal, A. Khawar, A. Abdel-Hadi, and T. C. Clancy, "Radar precoder design for spectral coexistence with coordinated multi-point (comp) system," *CoRR*, vol. abs/1503.04256, 2015.

[24] Federal Communications Commission (FCC), "FCC proposes innovative small cell use in 3.5 GHz band." Online: http://www.fcc.gov/document/ fcc-proposes-innovative-small-cell-use-35-ghz-band, December 12, 2012.

[25] Federal Communications Commission (FCC), "In the matter of revision of parts 2 and 15 of the commission's rules to permit unlicensed national information infrastructure (U-NII) devices in the 5 GHz band." MOO, ET Docket No. 03-122, June 2006.

[26] FCC (2004), "Second report and order: Promoting efficient use of spectrum through elimination of barrier to the development of secondary markets," Tech. Rep., FCC 04-167.

[27] A. Khawar, A. Abdel-Hadi, and T. C. Clancy, "MIMO radar waveform design for coexistence with cellular systems," in *IEEE International Symposium on Dynamic Spectrum Access Networks: SSPARC Workshop (IEEE DySPAN 2014—SSPARC Workshop)* (McLean, USA), April 2014.

[28] M. Ghorbanzadeh, A. Abdelhadi, and C. Clancy, "A utility proportional fairness resource allocation in spectrally radar-coexistent cellular networks," in *Military Communications Conference (MILCOM)*, 2014.

[29] S. Sengupta and M. Chatterjee, "An economic framework for dynamic spectrum access and service pricing," *networking*,

IEEE/ACM Transactions on, vol. 17, pp. 1200-1213, August 2009.

[30] M. Pan, F. Chen, X. Yin, and Y. Fang, "Fair profit allocation in the spectrum auction using the Shapley value," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pp. 1-6, November 2009.

[31] J. Zhang and Q. Zhang, "Stackelberg Game for Utility-Based Cooperative Cognitive Radio Networks," MobiHoc '09 (New York, NY, USA), pp. 2332, ACM, 2009.

[32] X. Zhou and H. Zheng, "TRUST: A general framework for truthful double spectrum auctions," in *INFOCOM 2009, IEEE*, pp. 999-1007, April 2009.

[33] J. Jia, Q. Zhang, Q. Zhang, and M. Liu, "Revenue Generation for Truthful Spectrum Auction in Dynamic Spectrum Access," MobiHoc '09 (New York, NY, USA), pp. 3-12, ACM, 2009.

[34] C.-C. Wu, C.-C. Chang, and I.-C. Lin, "New sealed-bid electronic auction with fairness, security and efficiency," *J. Comput. Sci. Technol.*, vol. 23, no. 2, pp. 253-264, 2008.

[35] K. Peng, C. Boyd, and E. Dawson, "Batch verification of validity of bids in homomorphic e-auction," *Comput. Commun.*, vol. 29, pp. 2798-2805, September 2006.

[36] M. Pan, J. Sun, and Y. Fang, "Purging the back-room dealing: Secure spectrum auction leveraging Paillier cryptosystem," in IEEE Journal on Selected Areas in Communications, vol. 29, no. 4, April 2011.

[37] V. Krishna, "Auction Theory," Academic Press, 2002.

[38] S. Gandhi, C. Buragohain, L. Cao, H. Zheng, and S. Suri, "A general framework for wireless spectrum auctions," in *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2007.

[39] M. Pan, F. Chen, X. Yin, and Y. Fang, "Fair profit allocation in the spectrum auction using the shapley value," in *Proceedings of the 28th IEEE Conference on Global Telecommunications*, 2009.

[40] S. de Vries and R. Vohra, "Combinatorial Auctions: A Survey," 2003.

[41] T. Groves, "Incentives in teams," in ECONOMETRICA, vol. 41, no. 4, pp. 617-631, July 1973.

[42] S. Gandhi, C. Buragohain, L. Cao, H. Zheng, and S. Suri, "A general framework for wireless spectrum auctions," in *DySPAN 2007*, pp. 22-33, April 2007.

[43] K. Jain, J. Padhye, V. N. Padmanabhan, and L. Qiu, "Impact of Interference on Multi-hop Wireless Network Performance," MobiCom '03 (New York, NY, USA), pp. 66-80, ACM, 2003.

[44] L. Chung, "Energy efficiency of QoS routing in multi-hop wireless networks," in *IEEE International Conference on Electro/Information Technology (EIT)*, 2010.

[45] X. Zhou, S. Gandhi, S. Suri, and H. Zheng, "eBay in the Sky: Strategy-proof Wireless Spectrum Auctions," MobiCom '08 (New York, NY, USA), pp. 2-13, ACM, 2008.

[46] L. B. Le, D. Niyato, E. Hossain, D. I. Kim, and D. T. Hoang, "QoS-aware and energy-efficient resource management in OFDMA femtocells," *IEEE Transactions on Wireless Communications*, vol. 12, pp. 180-194, January 2013.

[47] P. Klemperer, "Auction theory: A guide to the literature," in Journal of Economic Survey, vol. 13, no. 3, pp. 227-286, July 1999.

[48] K. Peng, C. Boyd, and E. Dawson, "Batch verification of validity of bids in homomorphic e-auction," in *Computer Communications*, vol. 29, no. 15, pp. 2798-2805, September 2006.

[49] J. Trevathan, "Security, anonymity and trust in electronic auctions," in *Crossroads*, vol. 11, no. 3, p. 2, May 2005.

[50] W. Vickrey, "Counterspeculation, auctions, and competitive sealed tenders," in The Journal of Finance, vol. 16, no. 1, pp. 8-37, March 1961.

[51] C. Wu, C. Chang, and I. Lin, "New sealed-bid electronic auction with fairness, security and efficiency," in Journal of Computer Science and Technology, vol. 23, pp. 253-264, 2008.

[52] M. Ghorbanzadeh, A. Abdelhadi, and C. Clancy, "Utility functions and radio resource allocation," in *Cellular Communications Systems in Congested Environments*, pp. 21-36, Springer, 2017.

[53] A. Best and B. Natarajan, "The effect of jamming on the performance of carrier interferometry/OFDM," in *Wireless and Mobile Computing, Networking and Communications. IEEE Int. Conf. on*, August 2005.

[54] J. Kim, D. G. An, H.-G. Ryu, and J. up Kim, "Analysis and design of SLM based DFT spreading OFDM system for active anti-jamming system," in *Radio and Wireless Symp. IEEE*, January 2011.

[55] L. Lightfoot, L. Zhang, and T. Li, "Performance of QO-STBC-OFDM in partial-band noise jamming," in *Information Sciences and Systems, 44th Annu. Conf.on,* pp. 1-6, March 2010. [56] M. Han, T. Yu, J. Kim, K. Kwak, S. Han, and D. Hong, "An efficient channel estimation algorithm under narrow-band jamming for OFDM systems," in *Military Communications Conference. IEEE,* October 2006.

[57] K. C. Beh, A. Doufexi, and S. Armour, "Performance evaluation of hybrid ARQ schemes of 3GPPLTE OFDMA system," in *Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on*, pp. 1-5, September.

[58] H. Shajaiah, A. Abdelhadi, and C. Clancy, "Utility functions and resource allocation for spectrum sharing," in *Resource Allocation with Carrier Aggregation in Cellular Networks*, pp. 19-24, Springer, 2018.

[59] M. Brady, M. Mohseni, and J. Cioffi, "Spatially-correlated jamming in Gaussian multiple access and broadcast channels," in *Information Sciences and Systems, 40th Annu. Conf. on*, March 2006.

[60] D. Chi and P. Das, "Effects of jammer and nonlinear amplifiers in MIMO-OFDM with application to 802.11n WLAN," in *Military Communications Conference. IEEE,* November 2008.

[61] Y. Cho, J. Kim, W. Yang, and C. Kang, "Mimo-OFDM Wireless Communications with Matlab," John Wiley & Sons, 2010.

[62] E. Jorswieck, H. Boche, and M. Weckerle, "Optimal transmitter and jamming strategies in Gaussian mimo channels," in *Vehicular Technology Conf. VTC 2005-Spring. IEEE 61st*, vol. 2, pp. 978-982, May 2005.

[63] D. Peng, L. Peng, C. Yin, and G. Yue, "The spatial diversity algorithms of carrier frequency offset synchronization for MIMO-OFDM systems," in *Wireless, Mobile and Multimedia Networks, 2006 IET International Conference on,* November 2006.

[64] M. Ghorbanzadeh, A. Abdelhadi, and C. Clancy, "Centralized resource allocation," in *Cellular Communications Systems in Congested Environments*, pp. 37-60, Springer, 2017.

[65] H. Ekstrom, "QoS control in the 3GPP evolved packet system," *Communications Magazine, IEEE,* vol. 47, pp. 76-83, February 2009.

[66] G. Intelligence, "Smartphone users spending more 'face time' on apps than voice calls or web browsing," 2011.

[67] N. S. Networks, "Understanding Smartphone Behavior in the Network," in Device Analyzer: Understanding Smartphone Usage, University of Cambridge, Cambridge, 2011.

[68] H. Shajaiah, A. Abdelhadi, and C. Clancy, "Multistage resource allocation with carrier aggregation," in *Resource Allocation with Carrier Aggregation in Cellular Networks*, pp. 25-62, Springer, 2018.

[69] M. Iwamura, K. Etemad, M.-H. Fong, R. Nory, and R. Love, "Carrier aggregation framework in 3GPP LTE-advanced [WiMAX/LTE Update]," *IEEE Communications Magazine*, vol. 48, no. 8, pp. 60-67, 2010.

[70] H. Shajaiah, A. Abdelhadi, and C. Clancy, "Resource allocation with carrier aggregation for commercial use of 3.5 GHz spectrum," in *Resource Allocation with Carrier Aggregation in Cellular Networks*, pp. 133-151, Springer, 2018.

[71] I. Research, "Mobile VoIP subscribers will near 410 million by 2015; VoLTE still a long way off," 2010.

[72] N. Solutions and Networks, "Enhance mobile networks to deliver 1000 times more capacity by 2020," 2013.

[73] H. Shajaiah, A. Abdelhadi, and C. Clancy, "Resource allocation with user discrimination for spectrum sharing," in *Resource Allocation with Carrier Aggregation in Cellular Networks*, pp. 63-131, Springer, 2018.

[74] Y. Wang, K. I. Pedersen, T. B. Sorensen, and P. E. Mogensen, "Utility Maximization in LTE-Advanced Systems with Carrier Aggregation," in *VTC Spring*, pp. 1-5, 2011.

[75] H. Shajaiah, A. Abdelhadi, and C. Clancy, *Resource Allocation with Carrier Aggregation in Cellular Networks: Optimality and Spectrum Sharing Using C++ and MATLAB.* Springer Publishing Company, Incorporated, 1st ed., 2018.

[76] L. B. Le, E. Hossain, D. Niyato, and D. I. Kim, "Mobility-aware admission control with QoS guarantees in OFDMA femtocell networks," in *2013 IEEE International Conference on Communications (ICC)*, pp. 2217-2222, June 2013.

[77] H. Shajaiah, A. Abdelhadi, and C. Clancy, "Introduction," in *Resource Allocation with Carrier Aggregation in Cellular Networks*, pp. 1-18, Springer, 2018.

[78] G. RP-091440, "Work Item Description: CarrierAggregation for LTE," December 2009.

[79] M. Iwamura, K. Etemad, M.-H. Fong, R. Nory, and R. Love, "Carrier aggregation framework in 3GPP LTE-advanced [WiMAX/LTE Update]," *Communications Magazine, IEEE*, vol. 48, pp. 60-67, August 2010.

[80] PCAST, "Final PCAST Spectrum Report," Tech. Rep., July 2012.

[81] R. Kurrle, "Resource allocation for smart phones in 4G LTE advanced carrier aggregation," Master Thesis, Virginia Tech, 2012.

[82] H. Shajaiah, A. Abdel-Hadi, and C. Clancy, "Utility proportional fairness resource allocation with carrier aggregation in 4G-LTE," in *Military Communications Conference, MILCOM 2013—2013 IEEE*, pp. 412-417, November 2013.

[83] H. Shajaiah, A. Khawar, A. Abdel-Hadi, and T. Clancy, "Resource allocation with carrier aggregation in LTE advanced cellular system sharing spectrum with s-band radar," in *Dynamic Spectrum Access Networks (DYSPAN), 2014 IEEE International Symposium on*, pp. 34-37, April 2014.

[84] H. Shajaiah, A. Abdelhadi, and C. Clancy, "A price selective centralized algorithm for resource allocation with carrier aggregation in LTE cellular networks," in *2015 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 813-818, March 2015.

[85] A. Khawar, A. Abdelhadi, and T. C. Clancy, "Channel modeling between seaborne MIMO radar and MIMO cellular system," *CoRR*, vol. abs/1504.04325, 2015.

[86] J. Li and P. Stoica, *MIMO Radar Signal Processing*. Wiley-IEEE Press, 2008.

[87] A. Khawar, A. Abdelhadi, and T. C. Clancy, "3D channel modeling between seaborne MIMO radar and MIMO cellular system," *CoRR*, vol. abs/1504.04333, 2015.

[88] F. Paisana, J. P. Miranda, N. Marchetti, and L. A. DaSilva, "Database-aided sensing for radar bands," in *IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN)*, pp. 1-6, April 2014.

[89] H. Deng and B. Himed, "Interference mitigation processing for spectrumsharing between radar and wireless communications systems," *IEEE Transactions on Aerospace and Electronic Systems,* vol. 49, no. 3, pp. 19111919, 2013.

[90] A. Khawar, A. Abdelhadi, and T. C. Clancy, "Coexistence analysis between radar and cellular system in LoS channel," *CoRR,* vol. abs/1506.07468, 2015.

[91] A. Abdelhadi and C. Clancy, "An optimal resource allocation with joint carrier aggregation in 4G-LTE," in *Computing, Networking and Communications (ICNC), 2015 International Conference on,* pp. 138-142, February 2015.

[92] H. Shajaiah, A. Abdelhadi, and T. C. Clancy, "Towards an application-aware resource scheduling with carrier aggregation in cellular systems," *IEEE Communications Letters,* vol. 20, pp. 129-132, January 2016.

[93] M. Ghorbanzadeh, A. Abdelhadi, and C. Clancy, "Spectrum-shared resource allocation," in *Cellular Communications Systems in Congested Environments,* pp. 147-178, Springer, 2017.

[94] J. Lee, R. Mazumdar, and N. Shroff, "Non-convex optimization and rate control for multi-class services in the internet," in IEEE/ACM Transactions on Networking, vol. 13, no. 4, pp. 827-840, September 2005.

[95] P. Yi, X. Dong, A. Iwayemi, C. Zhou, and S. Li, "Real-time opportunistic scheduling for residential demand response," *Smart Grid, IEEE Transactions on,* vol. 4, pp. 227-234, March 2013.

[96] A.-H. Mohsenian-Rad, V. Wong, J. Jatskevich, R. Schober, and A. LeonGarcia, "Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid," *Smart Grid, IEEE Transactions on,* vol. 1, pp. 320-331, December 2010.

[97] C. Joe-Wong, S. Sen, S. Ha, and M. Chiang, "Optimized day-ahead pricing for smart grids with device-specific scheduling flexibility," *Selected Areas in Communications, IEEE Journal on,* vol. 30, pp. 1075-1085, July 2012.

[98] J. H. Yoon, R. Baldick, and A. Novoselac, "Dynamic demand response controller based on real-time retail price for residential

buildings," *Smart Grid, IEEE Transactions on*, vol. 5, pp. 121-129, January 2014.

[99] S. Li, D. Zhang, A. Roget, and Z. O'Neill, "Integrating home energy simulation and dynamic electricity price for demand response study," *Smart Grid, IEEE Transactions on*, vol. 5, pp. 779-788, March 2014.

[100] R. Weber, "Auction Theory: By Vijay Krishna. Academic Press, 2002," *Games and Economic Behavior*, vol. 45, no. 2, pp. 488-497, 2003.

[101] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: A survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, pp. 1294-1312, Third Quarter 2015.

[102] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," *IEEE Internet of Things Journal*, vol. 1, pp. 372-383, October 2014.

[103] G. Intelligence, *From concept to delivery: The M2M market today.* https://goo.gl/yFmi5s. February 2014.

[104] A. Kumar, A. Abdelhadi, and T. C. Clancy, "A delay efficient multiclass packet scheduler for heterogeneous M2M uplink," *IEEE MILCOM*, 2016.

[105] A. Kumar, A. Abdelhadi, and T. C. Clancy, "An online delay efficient packet scheduler for M2M traffic in industrial automation," *IEEE Systems Conference*, 2016.

[106] F. Ennesser, *Security in machine-to-machine communication: The role ofthe telecommunication operator.* Tech. Rep., Cinterion - Gemalto, 2012.

[107] J. Latvakoski, M. Alay, H. Ganem, B. Jubeh, A. Iivari, J. Laguay, J. Bosch, and N. Granqvist, "Towards horizontal architecture for autonomic M2M service network," *Future Internet*, vol. 6, no. 2, pp. 261-301, 2014.

[108] E. J. M. Colbert and S. Hutchinson, *Intrusion Detection in Industrial Control Systems*, pp. 209-237. Cham: Springer International Publishing, 2016.

[109] M. Bishop, S. Cheung, and C. Wee, "The threat from the net [internet security]," *IEEE Spectrum*, vol. 34, pp. 56-63, August 1997.

[110] Y. Wu, B. Wang, K. Liu, and T. Clancy, "A multi-winner cognitive spectrum auction framework with collusion-resistant mechanisms," in *DySPAN 2008*, pp. 1-9, October 2008.

[111] F. Wu and N. Vaidya, "A strategy-proof radio spectrum auction mechanism in noncooperative wireless networks," *Mobile Computing, IEEE Transactions on*, vol. 12, pp. 885-894, May 2013.

[112] R. McAfee, "A dominant strategy double auction," *Journal ofEconomic Theory*, vol. 56, no. 2, pp. 434-450, 1992.

[113] D. Yang, X. Fang, and G. Xue, "Truthful Auction for Cooperative Communications," MobiHoc 11, (New York, NY, USA), pp. 9:1-9:10, ACM, 2011.

[114] X. Feng, Y. Chen, J. Zhang, Q. Zhang, and B. Li, "TAHES: A truthful double auction mechanism for heterogeneous spectrums," *Wireless Communications, IEEE Transactions on*, vol. 11, pp. 4038-4047, November 2012.

[115] Y. Chen, J. Zhang, K. Wu, and Q. Zhang, "TAMES: A truthful auction mechanism for heterogeneous spectrum allocation," in *INFOCOM, 2013 Proceedings IEEE*, pp. 180-184, April 2013.

[116] Q. Huang, Y. Tao, and F. Wu, "SPRING: A strategy-proof and privacy preserving spectrum auction mechanism," in *INFOCOM, 2013 Proceedings IEEE*, pp. 827-835, April 2013.

[117] W. Dong, S. Rallapalli, R. Jana, L. Qiu, K. Ramakrishnan, L. Razoumov, Y. Zhang, and T. W. Cho, "iDEAL: Incentivized dynamic cellular offloading via auctions," in *INFOCOM, 2013 Proceedings IEEE*, pp. 755-763, April 2013.

[118] X. Zhuo, W. Gao, G. Cao, and Y. Dai, "Win-Coupon: An incentive framework for 3G traffic offloading," in *Network Protocols (ICNP), 201119th IEEE International Conference on*, pp. 206-215, October 2011.

[119] Y. Zhang, D. Yang, J. Lin, M. Li, G. Xue, J. Tang, and L. Xie, "Spectrum auctions under physical interference model," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, pp. 719-728, December 2017.

[120] N. Saini and M. Chatterjee, "Multi-bid spectrum auctions in dynamic spectrum access networks with spatial reuse," in *2017 9th*

International Conference on Communication Systems and Networks (COMSNETS), pp. 101108, January 2017.

[121] M. Dong, G. Sun, X. Wang, and Q. Zhang, "Combinatorial auction with time-frequency flexibility in cognitive radio networks," in *INFOCOM, 2012 Proceedings IEEE*, pp. 2282-2290, March 2012.

[122] F. Wu and N. Vaidya, "SMALL: A strategy-proof mechanism for radio spectrum allocation," in *INFOCOM, 2011 Proceedings IEEE*, pp. 81-85, April 2011.

[123] M. Yokoo and K. Suzuki, "Secure multi-agent dynamic programming based on homomorphic encryption and its application to combinatorial auctions," in *Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems: Part 1*, AAMAS '02, (New York, NY, USA), pp. 112-119, ACM, 2002.

[124] K. Suzuki and M. Yokoo, "Secure Generalized Vickrey Auction using ho-momorphic encryption," in *Financial Cryptography* (R. N. Wright, ed.), vol. 2742 of *Lecture Notes in Computer Science*, pp. 239-249, Springer, 2003.

[125] M. Yokoo and K. Suzuki in *Financial Cryptography* (A. Juels, ed.), vol. 3110 of *Lecture Notes in Computer Science*, pp. 132-146, Springer, 2004.

[126] M. Pan, J. Sun, and Y. Fang, "Purging the back-room dealing: Secure spectrum auction leveraging paillier cryptosystem," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 866-876, 2011.

[127] G. Piro, L. Grieco, G. Boggia, and P. Camarda, "A two-level scheduling algorithm for QoS support in the downlink of LTE cellular networks," in *Wireless Conference (EW)*, 2010.

[128] G. Monghal, K. Pedersen, I. Kovacs, and P. Mogensen, "QoS oriented time and frequency domain packet schedulers for the UTRAN long term evolution," in *IEEE Vehicular Technology Conference (VTC)*, 2008.

[129] D. Soldani, H. X. Jun, and B. Luck, "Strategies for mobile broadband growth: Traffic segmentation for better customer experience," in *IEEE Vehicular Technology Conference (VTC)*, 2011.

[130] H. Ekstrom, A. Furuskar, J. Karlsson, M. Meyer, S. Parkvall, J. Torsner, and M. Wahlqvist, "Technical solutions for the 3G long-term

evolution," vol. 44, pp. 38-45, March 2006.
[131] F. Kelly, A. Maulloo, and D. Tan, "Rate control in communication networks: Shadow prices, proportional fairness and stability," in *Journal of the Operational Research Society,* vol. 49,1998.
[132] S. Low, F. Paganini, and J. Doyle, "Internet congestion control," *Control Systems, IEEE,* vol. 22, pp. 28-43, February 2002.
[133] S. H. Low and D. E. Lapsley, "Optimization flow control, I: Basic algorithm and convergence," *IEEE/ACM Transactions on Networking,* vol. 7, no. 6, pp. 861-874, 1999.
[134] J. Mo and J. Walrand, "Fair end-to-end window-based congestion control," *Networking, IEEE/ACM Transactions on,* vol. 8, pp. 556-567, October 2000.
[135] S. Shenker, "Fundamental design issues for the future internet," *Selected Areas in Communications, IEEE Journal on,* vol. 13, pp. 1176-1188, September 1995.
[136] Z. Cao and E. Zegura, "Utility max-min: An application-oriented bandwidth allocation scheme," in *INFOCOM '99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE,* vol. 2, pp. 793-801, March 1999.
[137] S. Sarkar and L. Tassiulas, "Fair allocation of utilities in multirate multicast networks: A framework for unifying diverse fairness objectives," *Automatic Control, IEEE Transactions on,* vol. 47, pp. 931-944, June 2002.
[138] H. Y. and S. Alamouti, "OFDMA: A broadband wireless access technology," in *IEEE SarnoffSymposium,* 2006.
[139] A. Larmo, M. Lindstrom, M. Meyer, G. Pelletier, J. Torsner, and H. Wiemann, "The LTE link-layer design," in IEEE Commun. Mag., vol. 47, no. 4, pp. 52-59, April 2009.
[140] C. Ciochina and H. Sari, "A review of OFDMA and single-carrier FDMA," in *Wireless Conference (EW),* 2010.
[141] C. Dovrolis, D. Stiliadis, and P. Ramanathan, "Proportional differentiated services: Delay differentiation and packet scheduling," in *IEEE/ACM Transactions on Networking,* vol. 10, no. 1, February 2002.
[142] A. Sali, A. Widiawan, S. Thilakawardana, R. Tafazolli, and B. Evans, "Cross-layer design approach for multicast scheduling over satellite

networks," in *Wireless Communication Systems, 2005. 2nd International Symposium on*, 2005.
[143] G. T. V9.0.0, "Further advancements for e-utra physical layer aspects," 2012.
[144] 3GPP Technical Report 36.211, "Physical Channels and Modulation," www.3gpp.org.
[145] 3GPP Technical Report 36.213, "Physical Layer Procedures," www.3gpp.org.
[146] European Telecommunications Standards Institute, "UMTS; LTE; UTRA; E-UTRA; EPC; UE conformance specification for UE positioning; Part 1: Conformance test specification," 2012.
[147] European Telecommunications Standards Institute, "UMTS; UTRA; General description; Stage 2," 2016.
[148] F. Li, "Quality of Service, Traffic Conditioning, and Resource Management in Universal Mobile Telecommunication System (UMTS)," 2003.
[149] FCC (2010), "Unlicensed operations in the TV broadcast bands, second memorandum opinion and order," Tech. Rep., FCC 10-174.
[150] IXIACOM, "Quality of Service (QoS) and Policy Management in Mobile Data Networks," 2010.
[151] M. Alasti, B. Neekzad, J. Hui, and R. Vannithamby, "Quality of service in WiMAX and LTE networks [Topics in Wireless Communications]," 2010.
[152] D. Niyato and E. Hossain, "Wireless broadband access: WIMAX and beyond—Integration of WiMAX and WiFi: Optimal pricing for bandwidth sharing," *IEEE Communications Magazine*, vol. 45, pp. 140-146, May 2007.
[153] J. Andrews, A. Ghosh, and R. Muhamed, "Fundamenytals of WiMAX: Understanding Broadband Wireless Netwroking," 2007.
[154] Z. Kbah and A. Abdelhadi, "Resource allocation in cellular systems for applications with random parameters," in *2016 International Conference on Computing, Networking and Communications (ICNC)*, pp. 1-5, February 2016.
[155] T. Erpek, A. Abdelhadi, and T. C. Clancy, "Application-aware resource block and power allocation for LTE," in *2016 Annual IEEE Systems Conference (SysCon)*, pp. 1-5, April 2016.

[156] S. Qaiyum, I. A. Aziz, and J. B. Jaafar, "Analysis of big data and quality-of-experience in high-density wireless network," in *2016 3rd International Conference on Computer and Information Sciences (ICCOINS)*, pp. 287-292, August 2016.

[157] A. Ghosh and R. Ratasuk, "Essentials of LTE and LTE-A," 2011.

[158] A. Abdel-Hadi and C. Clancy, "A utility proportional fairness approach for resource allocation in 4G-LTE," in *Computing, Networking and Communications (ICNC), 2014 International Conference on*, pp. 1034-1040, February 2014.

[159] A. Abdel-Hadi and C. Clancy, "A robust optimal rate allocation algorithm and pricing policy for hybrid traffic in 4G-LTE," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on*, pp. 2185-2190, September 2013.

[160] A. Abdel-Hadi, C. Clancy, and J. Mitola, III, "A resource allocation algorithm for users with multiple applications in 4G-LTE," in *Proceedings of the 1st ACM Workshop on Cognitive Radio Architectures for Broadband*, CRAB '13, (New York, NY, USA), pp. 13-20, ACM, 2013.

[161] H. Shajaiah, A. Abdel-Hadi, and C. Clancy, "Spectrum sharing between public safety and commercial users in 4G-LTE," in *Computing, Networking and Communications (ICNC), 2014 International Conference on*, pp. 674-679, February 2014.

[162] H. Shajaiah, A. Abdelhadi, and C. Clancy, "Multi-application resource allocation with users discrimination in cellular networks," in *2014 IEEE 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC)*, pp. 1163-1168, September 2014.

[163] M. Ghorbanzadeh, A. Abdelhadi, and C. Clancy, "A utility proportional fairness radio resource block allocation in cellular networks," *arXiv:1406.2630v1*, 2014.

[164] T. Erpek, A. Abdelhadi, and T. Clancy, "An optimal application-aware resource block scheduling in LTE," in *Computing, Networking and Communications (ICNC), 2015 International Conference on*, pp. 275-279, February 2015.

[165] M. Awad, V. Mahinthan, M. Mehrjoo, X. Shen, and J. W. Mark, "A dual-decomposition-based resource allocation for OFDMA networks with imperfect CSI," *Vehicular Technology, IEEE Transactions on*, vol. 59, pp. 2394-2403, June 2010.

[166] M. Mehrjoo, S. Moazeni, and X. S. Shen, "Resource allocation in OFDMA networks based on interior point methods," *Wireless Communications and Mobile Computing*, vol. 10, no. 11, pp. 1493-1508,2010.

[167] P. Tejera, W. Utschick, J. Nossek, and G. Bauch, "Rate balancing in multiuser MIMO OFDM systems," *Communications, IEEE Transactions on*, vol. 57, pp. 1370-1380, May 2009.

[168] L. Xu, X. Shen, and J. W. Mark, "Fair resource allocation with guaranteed statistical QoS for multimedia traffic in wideband CDMA cellular network," *Mobile Computing, IEEE Transactions on*, vol. 4, pp. 166-177, March 2005.

[169] M. Mehrjoo, M. Awad, M. Dianati, and X. Shen, "Design of fair weights for heterogeneous traffic scheduling in multichannel wireless networks," *Communications, IEEE Transactions on*, vol. 58, pp. 2892-2902, October 2010.

[170] R. Madan, S. Boyd, and S. Lall, "Fast algorithms for resource allocation in wireless cellular networks," *Networking, IEEE/ACM Transactions on*, vol. 18, pp. 973-984, June 2010.

[171] Y.-B. Lin, T.-H. Chiu, and Y.-T. Su, "Optimal and near-optimal resource allocation algorithms for OFDMA networks," *Wireless Communications, IEEE Transactions on*, vol. 8, pp. 4066-4077, August 2009.

[172] G. Li and H. Liu, "Downlink dynamic resource allocation for multi-cell OFDMA system," in *Signals, Systems and Computers, 2004. Conference Record of the Thirty-Seventh Asilomar Conference on*, vol. 1, pp. 517-521 Vol. 1, November 2003.

[173] S. Cicalo, V. Tralli, and A. Perez-Neira, "Centralized vs Distributed Resource Allocation in multi-cell OFDMA systems," in *Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd*, pp. 1-6, May 2011.

[174] M. Dianati, X. Shen, and K. Naik, "Cooperative fair scheduling for the downlink of CDMA cellular networks," *Vehicular Technology,*

IEEE Transactions on, vol. 56, pp. 1749-1760, July 2007.

[175] P.-L. Tsai, K.-J. Lin, and W.-T. Chen, "Downlink radio resource allocation with carrier aggregation in MIMO LTE-advanced systems," in *Communications (ICC), 2014 IEEE International Conference on*, pp. 2332-2337, June 2014.

[176] H. S. Liao, P. Y. Chen, and W. T. Chen, "An efficient downlink radio resource allocation with carrier aggregation in LTE-advanced networks," *IEEE Transactions on Mobile Computing*, vol. 13, pp. 2229-2239, October 2014.

[177] S. Rostami, K. Arshad, and P. Rapajic, "Optimum radio resource management in carrier aggregation based LTE-advanced systems," *IEEE Transactions on Vehicular Technology*, vol. PP, no. 99, pp. 1-1, 2017.

[178] L. P. Qian, Y. J. A. Zhang, J. Huang, and Y. Wu, "Demand response management via real-time electricity price control in smart grids," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 1268-1280, July 2013.

[179] P. Samadi, H. Mohsenian-Rad, V. W. S. Wong, and R. Schober, "Real-time pricing for demand response based on stochastic approximation," *IEEE Transactions on Smart Grid*, vol. 5, pp. 789-798, March 2014.

[180] L. Gkatzikis, I. Koutsopoulos, and T. Salonidis, "The role of aggregators in smart grid demand response markets," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 1247-1257, July 2013.

[181] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, pp. 81-85, January 2010.

[182] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *2010 First IEEE International Conference on Smart Grid Communications*, pp. 327-332, October 2010.

[183] N. Wang, T. Jiang, W. Li, and S. Lv, "Physical-layer security in internet of things based on compressed sensing and frequency selection," *IET Communications*, vol. 11, no. 9, pp. 1431-1437, 2017.

[184] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, pp. 1747-1761, October 2015.

[185] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for IoT under eavesdropper collusion," *IEEE Transactions on Automation Science and Engineering*, vol. 13, pp. 1281-1293, July 2016.

[186] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840-2853, 2016.

[187] J. Yue, C. Ma, H. Yu, and W. Zhou, "Secrecy-based access control for device-to-device communication underlaying cellular networks," *IEEE Communications Letters*, vol. 17, pp. 2068-2071, November 2013.

[188] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, "Interference exploitation in D2D-enabled cellular networks: A secrecy perspective," *IEEE Transactions on Communications*, vol. 63, pp. 229-242, January 2015.

[189] A. Sengupta, R. Tandon, and T. C. Clancy, "Fundamental limits of caching with secure delivery," *IEEE Transactions on Information Forensics and Security*, vol. 10, pp. 355-370, February 2015.

[190] F. Gabry, V. Bioglio, and I. Land, "On edge caching with secrecy constraints," in *2016 IEEE International Conference on Communications (ICC)*, pp. 1-6, May 2016.

[191] V. Bukac, P. Tucek, and M. Deutsch, "Advances and challenges in standalone host-based intrusion detection systems," in *Trust, Privacy and Secu-ritty in Digital Business* (S. Fischer-Hùbner, S. Katsikas, and G. Quirchmayr, eds.) (Berlin, Heidelberg), pp. 105-117, Springer Berlin Heidelberg, 2012.

[192] T. Sarkar and N. Das, *Survey on Host and Network Based Intrusion Detection System. Acta Technica Corviniensis—Bulletin of Engineering.* vol. 8, pp. 17-20, January 2015.

[193] A. Lakhina, M. Crovella, and C. Diot, "Mining anomalies using traffic feature distributions," *SIGCOMM Comput. Commun. Rev.*, vol. 35, pp. 217228, August 2005.

[194] S. Rajasegarar, C. Leckie, M. Palaniswami, and J. C. Bezdek, "Distributed anomaly detection in wireless sensor networks," in *2006 10th IEEE Singapore International Conference on Communication Systems*, pp. 1-5, October 2006.

[195] H. Wang, Z. Yuan, and C. Wang, "Intrusion detection for wireless sensor networks based on multi-agent and refined clustering," in *2009 WRI International Conference on Communications and Mobile Computing*, vol. 3, pp. 450-454, January 2009.

[196] P. Datta Kumar, *A Cloud Based Automated Anomaly Detection Framework.* Master's thesis, The University of Texas at Arlington. Texas, U.S.A, 2014.

[197] H. Sedjelmaci, S. M. Senouci, and M. Al-Bahri, "A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology," in *2016 IEEE International Conference on Communications (ICC)*, pp. 1-6, May 2016.

[198] A. Abdelhadi, H. Shajaiah, and C. Clancy, "A multitier wireless spectrum sharing system leveraging secure spectrum auctions," *Cognitive Communications and Networking, IEEE Transactions on*, no. 99, 2015.

[199] FCC, *Spectrum Policy Task Force Report.* Federal Communications Commission, Spectrum Policy Task Force, 2002.

[200] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Comput. Netw.*, vol. 50, pp. 2127-2159, September 2006.

[201] NTIA, "An assessment of the near-term viability of accommodating wireless broadband systems in the 1675-1710 MHz, 1755-1780 MHz, 3500-3650 MHz, 4200-4220 MHz and 4380-4400 MHz bands," 2010.

[202] National Telecommunications and Information Administration (NTIA), "Analysis and resolution of RF interference to radars operating in the band 2700-2900 MHz from broadband communication transmitters," Online, October 2012.

[203] Michael G. Cotton and Roger A. Dalke, "Spectrum occupancy measurements of the 3550-3650 megahertz maritime radar band near San Diego, California," 2014.

[204] A. Lackpour, M. Luddy, and J. Winters, "Overview of interference mitigation techniques between wimax networks and ground based radar," 2011.

[205] F. Sanders, J. Carrol, G. Sanders, and R. Sole, "Effects of radar interference on LTE base station receiver performance," 2013.

[206] M. P. Fitz, T. R. Halford, I. Hossain, and S. W. Enserink, "Towards simultaneous radar and spectral sensing," in *IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN)*, pp. 15-19, April 2014.

[207] Z. Khan, J. J. Lehtomaki, R. Vuohtoniemi, E. Hossain, and L. A. Dasilva, "On opportunistic spectrum access in radar bands: Lessons learned from measurement of weather radar signals," *IEEE Wireless Communications*, vol. 23, pp. 40-48, June 2016.

[208] S. S. Bhat, R. M. Narayanan, and M. Rangaswamy, "Bandwidth sharing and scheduling for multimodal radar with communications and tracking," in *IEEE Sensor Array and Multichannel Signal Processing Workshop*, pp. 233-236, 2012.

[209] R. Saruthirathanaworakun, J. Peha, and L. Correia, "Performance of data services in cellular networks sharing spectrum with a single rotating radar," in *IEEE International Symposium on a World ofWireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1-6,2012.

[210] C. Rossler, E. Ertin, and R. Moses, "A software defined radar system for joint communication and sensing," in *IEEE Radar Conference (RADAR)*, pp. 1050-1055, May 2011.

[211] R. Y. X. Li, Z. Zhang, and W. Cheng, "Research of constructing method of complete complementary sequence in integrated radar and communication," in *IEEE Conference on Signal Processing*, vol. 3, pp. 1729-1732,2012.

[212] P. Paillier, "Public-key cryptosystems based on composite degree residu-osity classes," *j-LECT-NOTES-COMP-SCI*, vol. 1592, pp. 223-238,1999.

[213] P. Paillier and D. Pointcheval, "Efficient public-key cryptosystems prov-ably secure against active adversaries," in *Proceedings ofthe International Conference on the Theory and Applications*

ofCryptology and Information Security: Advances in Cryptology, **AsIACRYPT** '99 (London, UK), pp. 165-179, Springer-Verlag, 1999.

[214] A. Khawar, A. Abdelhadi, and C. Clancy, "Target detection performance of spectrum sharing mimo radars," *Sensors Journal, IEEE*, vol. 15, pp. 49284940, September 2015.

[215] C. Sturm and W. Wiesbeck, "Waveform design and signal processing aspects for fusion of wireless communications and radar sensing," *Proceedings of the IEEE*, vol. 99, pp. 1236-1259, July 2011.

[216] C. Shahriar, A. Abdelhadi, and T. C. Clancy, "Overlapped-mimo radar waveform design for coexistence with communication systems," *CoRR*, vol. abs/1502.04117, 2015.

[217] X. Chen, X. Wang, S. Xu, and J. Zhang, "A novel radar waveform compatible with communication," in *International Conference on Computational Problem-Solving (ICCP)*, pp. 177-181,2011.

[218] A. Khawar, A. Abdelhadi, and T. Clancy, "A mathematical analysis of cellular interference on the performance of s-band military radar systems," in *Wireless Telecommunications Symposium (WTS), 2014*, pp. 1-8, April 2014.

[219] FCC (2003), "The development of secondary markets-report and order and further notice of proposed rule marketing," Tech. Rep., FCC 03-113.

[220] Federal Communications Commission, "Mobile Broadband: The Benefits of Additional Spectrum," 2010.

[221] J. Jose, A. Abdel-Hadi, P. Gupta, and S. Vishwanath, "On the impact of mobility on multicast capacity of wireless networks," in *INFOCOM, 2010 Proceedings IEEE*, pp. 1-5, March 2010.

[222] A. Abdel-Hadi and S. Vishwanath, "On multicast interference alignment in multihop systems," in *IEEE Information Theory Workshop 2010 (ITW 2010)*, 2010.

[223] T. Groves, "Incentives in teams," *Econometrica*, vol. 41, pp. 617-631, 1973.

[224] W. Vickrey, "Counterspeculation, auctions and competitive sealed tenders," *Journal ofFinance*, pp. 8-37, 1961.

[225] N. Nisan, T. Roughgarden, É. Tardos, and V. V. Vazirani, *Algorithmic Game Theory*. New York, NY, USA: Cambridge University Press, 2007.

[226] F. Xue and P. R. Kumar, "The number of neighbors needed for connectivity of wireless networks," *Wirel. Netw.*, vol. 10, pp. 169-181, March 2004.

[227] H. Shajaiah, A. Abdelhadi, and T. C. Clancy, "Robust resource allocation with joint carrier aggregation in multicarrier cellular networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 4, pp. 53-65, March 2018.

[228] H. Shajaiah, A. Abdelhadi, and C. Clancy, "Spectrum sharing approach between radar and communication systems and its impact on radar's detectable target parameters," in *Vehicular Technology Conference (VTC Spring), 2015 IEEE 81st*, pp. 1-6, May 2015.

[229] S. Wilson and T. Fischetto, "Coastline population trends in the United States: 1960 to 2008," in *U.S. Dept. of Commerce*, 2010.

[230] M. Ghorbanzadeh, A. Abdelhadi, and C. Clancy, "A utility proportional fairness bandwidth allocation in radar-coexistent cellular networks," in *Military Communications Conference (MILCOM)*, 2014.

[231] A. Abdelhadi and T. C. Clancy, "Network MIMO with partial cooperation between radar and cellular systems," in *2016 International Conference on Computing, Networking and Communications (ICNC)*, pp. 1-5, February 2016.

[232] F. Wilson, I. Wakeman, and W. Smith, "Quality of Service Parameters for Commercial Application of Video Telephony," 1993.

[233] M. Richards, J. Scheer, and W. Holm, "Principles of Modern Radar," 2010.

[234] A. Abdelhadi, A. Khawar, and T. C. Clancy, "Optimal downlink power allocation in cellular networks," *Physical Communication*, vol. 17, pp. 1-14, 2015.

[235] M. Ghorbanzadeh, A. Abdelhadi, and C. Clancy, "Resource allocation architectures traffic and sensitivity analysis," in *Cellular Communications Systems in Congested Environments*, pp. 93-116, Springer, 2017.

[236] M. Ghorbanzadeh, A. Abdelhadi, and C. Clancy, "A utility proportional fairness approach for resource block allocation in cellular networks," in *IEEE International Conference on Computing, Networking and Communications (ICNC)*, 2015.

[237] H. Shajaiah, A. Abdelhadi, and C. Clancy, "RA with CA for a cellular system sharing spectrum with s-band radar," in *Resource Allocation with Carrier Aggregation in Cellular Networks*, pp. 153-172, Springer, 2018.

[238] H. Shajaiah, A. Abdelhadi, and C. Clancy, "Utility proportional fairness resource block scheduling with carrier aggregation," in *Resource Allocation with Carrier Aggregation in Cellular Networks*, pp. 173-188, Springer, 2018.

[239] D. Bertsekas, *Nonlinear Programming.* Athena Scientific Optimization and Computation Series, Athena Scientific, 2016.

[240] D. Bertsimas and J. Tsitsiklis, *Introduction to Linear Optimization.* Athena Scientific, 1st ed., 1997.

[241] J.-W. Lee, R. R. Mazumdar, and N. B. Shroff, "Downlink power allocation for multi-class wireless systems," *IEEE/ACM Trans. Netw.*, vol. 13, pp. 854867, August 2005.

[242] A. Parekh and R. Gallager, "A generalized processor sharing approach to flow control in integrated services networks: The single-node case," 1993.

[243] A. Demers, S. Keshav, and S. Shenker, "Analysis and simulation of a fair queueing algorithm," in ACM SIGCOMM Computer Communication Review, 1989.

[244] G. Tychogiorgos, A. Gkelias, and K. K. Leung, "Utility-proportional fairness in wireless networks," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2012 IEEE 23rd International Symposium on*, pp. 839-844, September 2012.

[245] A. Abdelhadi and T. C. Clancy, "Optimal context-aware resource allocation in cellular networks," in *2016 International Conference on Computing, Networking and Communications (ICNC)*, pp. 1-5, February 2016.

[246] M. Ghorbanzadeh, A. Abdelhadi, and C. Clancy, "Distributed resource allocation," in *Cellular Communications Systems in Congested Environments*, pp. 61-91, Springer, 2017.

[247] Y. Wang and A. Abdelhadi, "A QoS-based power allocation for cellular users with different modulations," in *2016 International Conference on Computing, Networking and Communications (ICNC)*, pp. 1-5, February 2016.

[248] M. Ghorbanzadeh, A. Abdelhadi, and C. Clancy, "Radio resource block allocation," in *Cellular Communications Systems in Congested Environments*, pp. 117-146, Springer, 2017.

[249] M. Ghorbanzadeh, A. Abdelhadi, A. Amanna, J. Dwyer, and T. Clancy, "Implementing an optimal rate allocation tuned to the user quality of experience," in *Computing, Networking and Communications (ICNC), 2015 International Conference on*, pp. 292-297, February 2015.

[250] A. Abdelhadi and H. Shajaiah, "Optimal resource allocation for cellular networks with MATLAB instructions," *CoRR*, vol. abs/1612.07862,2016.

[251] S. Boyd and L. Vandenberghe, *Convex Optimization.* New York, NY, USA: Cambridge University Press, 2004.

[252] D. Bertsekas, A. Nedic, and A. Ozdaglar, *Convex Analysis and Optimization.* Athena Scientific Optimization and Computation Series, Athena Scientific, 2003.

[253] A. Abdelhadi and C. Clancy, "An optimal resource allocation with joint carrier aggregation in 4G-LTE," in *Computing, Networking and Communications (ICNC), 2015 International Conference on*, pp. 138-142, February 2015.

[254] H. Shajaiah, A. Abdelhadi, and C. Clancy, "An optimal strategy for determining true bidding values in secure spectrum auctions," *IEEE Systems Journal*, vol. 13, pp. 1190-1201, June 2019.

[255] H. Shajaiah, A. Abdelhadi, and C. Clancy, "Conclusion and future trajectory," in *Resource Allocation with Carrier Aggregation in Cellular Networks*, pp. 189-191, Springer, 2018.

[256] G. Yuan, X. Zhang, W. Wang, and Y. Yang, "Carrier aggregation for LTE-advanced mobile communication systems," in *Communications Magazine, IEEE*, vol. 48, pp. 88-93, 2010.

[257] M. Ghorbanzadeh, A. Abdelhadi, and C. Clancy, "Optimal radio resource allocation for hybrid traffic in cellular networks: Traffic analysis and implementation," *CoRR*, vol. abs/1411.4012, 2014.

[258] Y. Wang, K. Pedersen, P. Mogensen, and T. Sorensen, "Resource allocation considerations for multicarrier LTE-advanced systems operating in backward compatible mode," in *Personal, Indoor and*

Mobile Radio Communications, 2009 IEEE 20th International Symposium on, pp. 370-374,2009.

[259] M. Ghorbanzadeh, A. Abdelhadi, and C. Clancy, "Optimal radio resource allocation for hybrid traffic in cellular networks: Centralized and distributed architecture," *CoRR*, vol. abs/1411.4011,2014.

[260] G. Tychogiorgos, A. Gkelias, and K. Leung, "A new distributed optimization framework for hybrid adhoc networks," in *GLOBECOM Workshops*, 2011.

[261] G. Tychogiorgos, A. Gkelias, and K. Leung, "Towards a fair non-convex resource allocation in wireless networks," in *IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2011.

[262] T. Jiang, L. Song, and Y. Zhang, Orthogonal Frequency Division Multiple Access Fundamentals and Applications, *Auerbach Publications*, 2010.

[263] S. Boyd and L. Vandenberghe, *Introduction to Convex Optimization with Engineering Applications.* Cambridge University Press, 2004.

[264] H. Tuy, *Convex Analysis and Global Optimization.* Springer Publishing Company, Incorporated, 2nd ed., 2016.

[265] D. Bertsekas and M. I. of Technology, *Convex Optimization Algorithms.* Athena Scientific, 2015.

[266] S. Shenker, "Fundamental design issues for the future internet," in IEEE Journal of Selected Area, vol. 13, no. 7, pp. 1176-1188, September 1995.

[267] H. Kushner and P. Whiting, "Convergence of proportional-fair sharing algorithms under general conditions," *IEEE Transactions on Wireless Communications*, vol. 3, no. 4, pp. 1250-1259, August 2004.

[268] M. Andrews, K. Kumaran, K. Ramanan, A. Stolyar, P. Whiting, and R. Vi-jayakumar, "Providing quality of service over a shared wireless link," in IEEE Communications Magazine, vol. 39, no. 2, pp. 150-154, February 2001.

[269] H. Shajaiah, A. Abdelhadi, and T. C. Clancy, "An efficient multicarrier resource allocation with user discrimination framework for 5G wireless systems," *Springer International Journal ofWireless Information Networks*, vol. 22, no. 4, pp. 345-356, 2015.

[270] Y. Wang, A. Abdelhadi, and T. C. Clancy, "Optimal power allocation for LTE users with different modulations," in *2016 Annual IEEE Systems Conference (SysCon)*, pp. 1-5, April 2016.

[271] H. Shajaiah, A. Abdelhadi, and C. Clancy, "Secure power scheduling auction for smart grids using homomorphic encryption," in *2017 IEEE International Conference on Big Data (Big Data)*, pp. 4507-4512, December 2017.

[272] H. Shajaiah, A. Sengupta, A. Abdelhadi, and C. Clancy, "Performance trade-offs in IoT uplink networks under secrecy constraints," in *2019 IEEE 30th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC Workshops)*, pp. 1-6, September 2019.

[273] A. Shokrollahi, "Raptor codes," *Information Theory, IEEE Transactions on*, vol. 52, pp. 2551-2567, June 2006.

[274] H. Zhou, X. Wang, Z. Liu, X. Zhao, Y. Ji, and S. Yamada, "QoS-aware resource allocation for multicast service over vehicular networks," in *2016 8th International Conference on Wireless Communications Signal Processing (WCSP)*, pp. 1-5, October 2016.

[275] Z. Fan, Y. Li, G. Shen, and C. C. K. Chan, "Dynamic resource allocation for all-optical multicast based on sub-tree scheme in elastic optical networks," in *2016 Optical Fiber Communications Conference and Exhibition (OFC)*, pp. 1-3, March 2016.

[276] S. Gao and M. Tao, "Energy-efficient resource allocation for multiple description coding based multicast services in OFDMA networks," in *2016IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 1-6, July 2016.

[277] S. Chieochan and E. Hossain, "Downlink media streaming with wireless fountain coding in wireline-cum-WiFi networks," *Wirel. Commun. Mob. Comput.*, vol. 12, pp. 1567-1579, December 2012.

[278] A. Abdelhadi, F. Rechia, A. Narayanan, T. Teixeira, R. Lent, D. Benhaddou, H. Lee, and T. C. Clancy, "Position estimation of robotic mobile nodes in wireless testbed using GENI," *CoRR*, vol. abs/1511.08936,2015.

[279] S. Chieochan and E. Hossain, "Wireless fountain coding with IEEE 802.11e block ACK for media streaming in wireline-cum-WiFi

networks: A performance study," *IEEE Transactions on Mobile Computing*, vol. 10, pp. 14161433, October 2011.

[280] S. Chieochan and E. Hossain, "Network coding for unicast in a WiFi hotspot: Promises, challenges, and testbed implementation," *Comput. Netw.*, vol. 56, pp. 2963-2980, August 2012.

[281] J. Chen, S. Olafsson, and X. Gu, "Observations on using simulated annealing for dynamic channel allocation in 802.11 wlans," in *IEEE Vehicular Technology Conference (VTC)*, 2008.

[282] A. Kumar, A. Abdelhadi, and C. Clancy, "Novel anomaly detection and classification schemes for machine-to-machine uplink," in *2018 IEEE International Conference on Big Data (Big Data)*, pp. 1284-1289, December 2018.

[283] A. Kumar, A. Abdelhadi, and T. C. Clancy, "A delay optimal MAC and packet scheduler for heterogeneous M2M uplink," *CoRR*, vol. abs/1606.06692, 2016.

[284] A. Kumar, A. Abdelhadi, and T. C. Clancy, "A delay-optimal packet scheduler for M2M uplink," *IEEE MILCOM*, 2016.

[285] A. Kumar, A. Abdelhadi, and T. C. Clancy, "A delay efficient MAC and packet scheduler for heterogeneous M2M uplink," *IEEE GLOBECOM Workshop on Internet of Everything (IoE)*, 2016.

[286] H. S. Dhillon, H. Huang, H. Viswanathan, and R. A. Valenzuela, "Fundamentals of throughput maximization with random arrivals for M2M communications," *IEEE Transactions on Communications*, vol. 62, pp. 40944109, November 2014.

[287] S. Ali and M. Zeeshan, "A delay-scheduler coupled game theoretic resource allocation scheme for LTE networks," in *Frontiers of Information Technology (FIT)*, 2011.

[288] D. Fudenberg and J. Tirole, "Nash equilibrium: Multiple Nash equilibria, focal points, and Pareto optimality," in *MIT Press*, 1991.

[289] P. Ranjan, K. Sokol, and H. Pan, "Settling for less—A QoS compromise mechanism for opportunistic mobile networks," in *SIGMETRICS Performance Evaluation*, 2011.

[290] R. Johari and J. Tsitsiklis, "Parameterized Supply Function Bidding: Equilibrium and Efficiency," 2011.

Index

Note: Page numbers followed by *f* denote figures; by *t*, tables.

A

Algorithm, 12. *See also* Distributed RA algorithm
  (1) MTSSA frequency bands allocation, 30, 31, 56
  (2) *i*th UE, 57, 58
  (3) *l*th eNodeB, 59
  (4) *k*th BS optimal bidding, 81–82, 89, 91–92, 92f
  (5) spectrum band allocation, 86–87, 89, 91–92, 92*f*
  convergence analysis issues with, 54–59
  distributed optimization, 53–55, 54*f*
Anomaly detection and classification, 13–14
  DDoS in, 122–123, 124, 125f, 126f, 129*t*
  device failure in, 123–124, 126, 128f, 129, 129f, 129*t*
  emergency scenario in, 123, 126, 127f, 129*t*
  M2M uplink communications, 124, 125f–129f, 126, 129–130, 129*t*
  at MAs, 120–121, 120*f*
  with MCD, 8, 119–121
AS. *See* M2M application server
Attack models, 117
  MDS against, 114
  passive eavesdropper, backhaul
  network, and, 107, 108f, 114–115, 116f, 132
Auction. *See* Power scheduling auction;
  Spectrum auction;
  Vickrey-Clarke-Groves (VCG) auction
Auctioneer:
  auction performed by, 30, 34
  BSs, and, 23, 29

in CSL, 36
determination of maximum bidding by, 31
greedy bidder and bid-rigging with, 6–7, 27, 27f, 39, 85
as grid operator, 97–98, 101–104, 104*f*
interference conflict graph by, 29
limitations on, 30, 39, 99, 101–103
private and public keys generated by, 32, 85, 102
revenue of, 20, 24, 34–36, 37f, 38, 39f, 74, 88, 93, 94f, 105, 105*f*
secure spectrum auction performed by, 30
spectrum allocation by, 33
underutilized frequency bands of, 21f, 22, 29, 34, 72, 93, 94*f*

B

Backhaul network:
in industrial IoT networks, 109, 111–115, 116f, 117
latency-limited, 108, 109, 111, 113–114, 115, 116f, 117
passive eavesdropper, attack models, and, 107, 108f, 114–115, 116f, 132
rate-limited, 111–113, 115, 116f, 117
Backroom dealing, 3, 6–7, 28
Base stations (BSs), 12
auctioneer, pilot channel, and, 23
bidder as, 3–4, 71
bidding value and location of, 35
coverage radius of, 22, 22*f*
k, 79–81, 84
*k*th optimal bidding algor*i*thm, 81–82,
89, 91–92, 92*f*
local conflict-table of, 29
macro cells, WSPs, and, 20, 21f–23f, 22, 34–35
non-adjacent carrier aggregation in, 71
permanent resources of, 71–73, 75
price per unit bandwidth of, 79, 90
root, 29, 30, 33–34, 86

shadow price calculated by, 89–90, 90*f*
small cells, WSPs, and, 20, 21f–23f, 22, 34–35
spectrum auction participation by, 72, 75–77
temporary resource seeking, 71–72, 75, 77
winning, 86
WSPs, and underutilized frequency bands, 20, 21f–23f, 22, 34–35
Bid-rigging, 3
greedy bidders and auctioneers in, 6–7, 27, 27f, 39, 85
in power scheduling auction, 101–102
prevention of, 10, 19, 34, 39
in SPRING, 39
in VCG auctions, 27, 27f, 100
Bidder satisfaction, 35
EPU increasing with, 105, 106*f*
with frequency band increase, 36, 38*f*
spectrum utilization, auctioneer revenue, and, 34, 88, 93, 94*f*
Bidding prices, final allocated rates of, 89–90, 90f, 92, 92f. *See also* True bidding price
demand-based compared to traditional bidding in, 91, 91*f*
in sigmoidal and logar*i*thmic utility functions in, 88, 89f, 89*t*
Bidding strategy, secure spectrum auctions, 71, 95
bidding prices, final allocated rates and, 88–92, 89f, 89t, 90f, 91f, 92*f*
BSs and, 72, 75–77
interference conflict graph used for, 75–76, 75*f*
key symbols in this chapter, 74*t*
Bidding strategy, secure spectrum logar*i*thmic or sigmoidal-like utility functions in, 82–84, 88, 89f, 89*t*
numerical results of, 88–93, 89f, 89t, 90f, 91f, 92f, 94*f*

spectrum band allocation in, 85–87
spectrum sharing, secure and truthful auctions in, 76–87, 76*f*
spectrum utilization, auctioneer revenue, and bidder satisfaction, 88, 93, 94*f*
system model for, 73–76, 74t, 75*f*
true bidding value in, 77–85
UPF RA optimization problem in, 78–80
Bidding value, 35. *See also* True bidding value
BS *k* calculating, 80–81
gateway randomizing encrypted, 32, 39, 71, 106
maximum for, 31–32
Paillier cryptosystem encrypting, 30–32
SPRING submission of, 38
THEMIS, frequency bands, and, 10
as traffic-dependent, 64, 65, 99
BS k:
bidding calculated by, 80–81, 84
optimal bidding algorithm, 81–82, 89, 91–92, 92*f*
UPF RA with CA used with, 79–80
BS n, 25, 31, 73
BSs. *See* Base stations

C

Carrier aggregation (CA), 50. *See also* Joint carrier aggregation, IoT, spectrum sharing systems; RA with joint CA
contiguous and noncontiguous, 4–6, 44
multistage RA using, 11, 44–45, 64–65, 64*f*
RA of, 2, 5–6, 14, 43, 71, 73
UPF, RA, and, 5, 79–80
CCs. *See* Component carriers
Ciphertext:
homomorphic addition,

indistinguishability, and self-blinding in, 28–29
Paillier cryptosystem leveraging, 19
in probabilistic encryption, 28
vector of, 31
Commercial spectrum bands, 2, 8
Component carriers (CCs), 4, 12
Concave natural logar*i*thms, 47–50
Conflict table, 29, 85–86
Connectivity, 109, 113, 115
Conventional spectrum leasing (CSL), 35
performance evaluation of, 36, 37f–38f, 41
Convergence analysis:
algor*i*thm drawbacks in, 54–57
algor*i*thm solutions in, 57–59
Convex optimization, 5, 44
multicarrier RA with CA optimization
problem as, 44, 50
as optimization problem, 47–50, 78, 80
Cryptography, 13. *See also* Paillier cryptosystem
CSL. *See* Conventional spectrum leasing Cyber-threat:
IDS reducing, 7–8, 119–120
in M2M, 2–3, 7, 13–14

D

Data collection process, IoT, 13
DDoS. *See* Distributed denial of service
Decodability constraint, 110–111, 112
Delay-tolerant applications, 59, 60*f*
in HetNet1, 63–64
in HetNet2, 65, 69
true bidding with, 88–89
Design:
in smart grids, 98, 99–101, 99*f*

in spectrum sharing systems, IoT, leveraging secure spectrum auctions, 26–28, 27*f*
Device failure, 8, 123–124
with feature-based detection, 129, 129f, 129*t*
with global volumetric detection, 129*t*
with local volumetric detection, 126, 128f, 129*t*
in M2M uplink communications, 119–120, 123–124
Distributed denial of service (DDoS), 3, 8, 119, 122
and emergency scenario with MCD, 123, 126, 128f, 133
with feature-based detection, 124, 126f, 129*t*
with global volumetric detection, 124, 125f, 129*t*
with local volumetric detection, 124, 125f, 129*t*
Distributed RA algorithm, 44, 45, 54, 54f, 55
fluctuation decay function in, 57–58
QoS in, 69
zero rate aversion in, 53
Downlink communications, IoT, 7, 13
Dual problem, 51–52

E

Eavesdropper, passive, 2
uplink networks attacked by, 107, 108f, 114–115, 116f, 132
Economic auction properties, 6–7, 27
incentive compatibility in, 24–26
individual rationality in, 24–26
no positive transfers in, 24–26
social welfare with, 25–26, 100
Electric power units (EPUs):
auctioneer determining, 98
auctioneer revenue, bidder satisfaction, and, 105, 105*f*
Emergency scenario, 8
DDoS with MCD, 123, 126, 128f, 133

with feature-based detection, 123, 126, 127f, 129*t*
with global volumetric detection, 126, 129*t*
with local volumetric detection, 126, 127f, 129*t*
in M2M uplink communications, 119–120, 121, 123
Encoding policy, 109–110
Encrypted bidding value, 71
federal gateway randomizing, 32, 39, 106
by Paillier cryptosystem, 30–32
eNodeB. *See* Evolve node B
EPUs. *See* Electric power units
Evolve node B (eNodeB), 4
allocation among mobile users, 11
in cellular cell, 45
convergence analysis, algor*i*thms, and, 54–59
in distributed RA algor*i*thm, 53
fluctuation decay function in, 58
in HetNet1, 60, 62f, 63–64, 63*f*
*l*th, 53–54, 59
optimization problem of, 52
of small cells at underutilized spectrum band, 59
UEs served by, 45

F

FCC. *See* Federal Communications Commission
Feature-based detection, 121
DDoS with, 124, 126f, 129*t*
device failure with, 129, 129f, 129*t*
emergency scenario with, 123, 126, 127f, 129*t*
in IT and M2M networks, 119
traffic anomaly scheme using, 13, 122–123
Federal Communications Commission (FFC), 4
radio spectrum management controlled by, 3, 8

secondary spectrum market legalized by, 8–9, 17
Federal gateway, 33, 41, 76*f*
randomizing encrypted bidding values by, 32, 39, 106
Federal government leasing, 18, 73
Fluctuation decay function, 57–58
Forwarding policy, 109, 110–111
Fourth-generation (4G) systems, 4
Fraud:
MTSSA avoiding, 34, 39
in power scheduling auction, 101–102
in spectrum band allocation, 85
in SPRING, 39
in VCG auctions, 26–28, 27f, 100
Frequency band, 4, 10, 36, 38f.
See also Underutilized frequency bands
Frequency band allocation:
auctioneer performing secure auction for, 30
interference property graph in, 29
MTSSA, 30, 31, 56
in secure spectrum auction design,
MTSSA, 29–30
Frequency conflict graph, 34, 36, 41, 132
of spectrum auction model, 22–23, 22f, 75*f*
subnet in WSPs, 22f, 23, 75*f*
Frequency reuse property, 10
BSs certain coverage radius, 22, 22*f*
in HetNet2, 65, 66*f*

H

Hessian matrix (H):
of logar*i*thmic utility function, 47–48
of sigmoidal-like utility function, 47, 49–50
Heterogeneous networks (HetNets).

See also HetNet1; HetNet2
simulation setup of, 59–69, 61f– 64f, 62t, 66f–68f, 66*t*
UE applications for, 60, 62*t*
HetNet1:
macro cell and small cell eNodeBs in, 60, 62f, 63–64, 63*f*
multistage RA with CA in, 64–65, 64*f*
RA with joint CA in, 60, 62f, 63–65, 64f, 67
rate allocation in, 60, 62f, 63–64, 63*f*
rate pricing analysis and comparison, 64–65, 64*f*
real-time and delay-tolerant
applications in, 63–64
system model for, 60, 61*f*
traffic-dependent pricing in, 65
zero rate in, 62f, 63
HetNet2:
frequency reuse property in, 65, 66*f*
rate allocation in, 66, 67f, 68*f*
real-time and delay-tolerant
applications in, 65, 69
system model for, 65, 66*f*
UPF in, 67, 67f–68f, 69
utility function parameters in, 65, 66*t*
zero rate in, 67, 67f–68f
Homomorphic encryption, 10, 29
of Paillier cryptosystem, 28, 32, 33, 41, 71, 85, 101
smart grid security scheme using, 12, 15
smart grids, communication using, 97, 99f, 101–103, 104f, 105–106, 105f, 106*f*

I

IDS. *See* Intrusion detection scheme
Incentive compatibility, 24–26
Individual rationality, 24–26

Industrial IoT networks:
backhaul network in, 109, 111–115, 116f, 117
central server in, 107, 109–110, 111–112, 113
latency-limited, 108, 109, 111, 113–114, 115, 116f, 117, 132
model for, 108–111, 108*f*
Interference conflict graph:
by auctioneer, 29
by secure gateway, 75–76, 75*f*
of spectrum auction model, 20, 21f, 22
Interference property, 10
Internet of Things (IoT), 13. *See also* Joint carrier aggregation, IoT, spectrum sharing systems; MATLAB; Spectrum sharing systems, IoT, leveraging secure spectrum auctions; specific *topics*
definition of, 1
Intrusion detection scheme (IDS), 13, 130
cyber-threat reduction using, 7–8, 119–120
IoT. *See* Internet of Things

J

Joint carrier aggregation, IoT, spectrum sharing systems, 43
convergence analysis of, 54–59
distributed optimization algor*i*thm of, 53–55, 54*f*
dual problem of, 51–52
global optimal solution for, 46–50, 56
HetNet1, 60, 61f–64f, 63–65
HetNet2, 65–67, 66f–68f, 66t, 69
Joint carrier aggregation, IoT, spectrum
multistage resource allocation using, 44–45
numerical results of, 59–69, 60f– 64f, 62t, 66f–68f, 66*t*
problem formation in, 45–46

RA optimization problem with, 44–45, 46, 50, 52
utility-proportional fairness in, 44–46

K

K-means, anomaly detection using, 14

L

Lagrange multiplier, 51, 52, 56. *See also* Shadow price
LAP. *See* Local access point
Latency-limited backhaul network, 108, 109, 111
backhaul rate vs. processing time, 115, 116f, 117
optimization problem in, 113–114
Local access point (LAP):
active attacks from IoT classes by rogue, 117, 133
encoding policy at, 109–110
MDS used by, 110
with SAPs, 107, 108f, 109, 111
sensor data encoded at, 110
Logarithm, natural, 48
of concave and convex optimization, 47–50
of sigmoidal-like utility function, 50, 55–56
Logarithmic utility function:
Hessian matrix of, 47–48
real-time application simulated by, 59, 60*f*
in true bidding values, 82–84, 88, 89
in UPF, 44–45, 77–78
Long-Term Evolution (LTE), 45
CA, 4G, and, 4, 59
optimal rate allocation in, 54
QoS of, 46
LTE third-generation partnership project

(3GPP), 11

M

M2M. *See* Machine-to-machine
M2M aggregators (MAs):
anomaly detection at, 120–121, 120*f*
M2M uplink system consisting of, 8
M2M application server (AS), 8, 120–121, 120*f*
M2M AS. *See* M2M application server
M2M uplink communications, 8, 15
anomaly detection and classification for, 124, 125f–129f, 126, 129–130, 129*t*
anomaly metrics in, 121–122
emergency scenario in, 119–120, 121, 123
MCD in, 119–120
numerical results for, 124, 125f–129f, 126, 129–130, 129*t*
system model for, 120–121, 120*f*
terminal device failure in, 119–120, 123–124
Machine-to-machine (M2M), 119. *See also* M2M uplink communications
cyber-threats in, 2–3, 7, 13–14
DDoS attacks, emergency scenarios,
and terminal device failure in, 8
physical-layer security methods with, 7
Machine-type communications (MTCs), 1
Macro cells, 132
BSs, WSPs, and, 20, 21f–23f, 22, 34–35
eNodeB at LTE-Advanced of, 59
in HetNet1, 60, 62f, 63–64, 63*f*
MAs. *See* M2M aggregators
MATLAB:
for IoT smart grid, 147–151
for IoT spectrum sharing, 135–145

simulation of logar*i*thmic,
sigmoidal-like utility functions,
and, 59
Maximum distance separable (MDS), 110, 114
McAfee mechanism, 9
MCD. *See* Modified Canberra distance metric
MCSs. *See* Modulation and coding schemes
MIMO radar carrier, 5
Modified Canberra distance metric (MCD):
anomaly detection scheme with, 8, 119–121
DDoS and emergency scenario with, 123, 126, 128f, 133
Modulation and coding schemes (MCSs), 12
Monte Carlo simulations, 8, 35, 93, 105, 120, 124
MTCs. *See* Machine-type communications
MTSSA, 10
contributions of, 18–19
fraud avoiding, 34, 39
frequency band allocation, 30, 31, 56
Paillier cryptosystem leveraged by, 28–34, 39, 41
payment method of, 19, 38
performance evaluation of, 34–39, 37f–38f, 39*f*
properties of, 14
as secure spectrum auction, 3–4, 18, 28–34, 76, 131
security and complexity analysis of, 39–41, 40t, 41*f*
spectrum auction model for, 23, 23*f*
spectrum reusability and secure auction in, 36, 37f–38f, 72
SPRING compared to, 38–39, 39*f*
THEMIS compared to, 40, 40t, 41*f*
MTSSA-FL. *See* MTSSA with fixed limit
MTSSA with fixed limit (MTSSA-FL):
as auction mechanism, 34

performance evaluation with, 35–36, 37f–38f
Multicarrier cellular network, 11–12, 44, 50
Multicarrier RA with CA optimization
problem, 44, 50–52
Multistage RA, 5
CA in, 11, 44–45, 64–65, 64*f*

N

National Broadband Plan (NBP), 4
NBP. *See* National Broadband Plan
Networked TCP/IP architecture, 7
Neural networks, 14
Non-adjacent carrier aggregation, 71
NP-complete, 3, 9
Numerical results and analysis:
of bidding strategy, secure spectrum
auctions, 88–93, 89f, 89t, 90f–92f, 94*f*
of joint carrier aggregation, IoT,
spectrum sharing systems, 59–69, 60f–64f, 62t, 66f–68f, 66*t*
for M2M uplink communications, 124, 125f–129f, 126, 129–130, 129*t*
performance analysis of, 34–39, 37f–39f, 93, 94*f*
of smart grids, communication using
homomorphic encryption, 104–106, 105f, 106*f*
of spectrum sharing systems, IoT,
leveraging secure spectrum
auctions, 34–41, 37f–39f, 40t, 41*f*
spectrum utilization, auctioneer
revenue, and bidder satisfaction in, 34, 93, 94*f*
spectrum utilization vs. auctioneer
available underutilized bands, 93, 94*f*
of uplink networks secrecy, IoT, 115, 116f, 117

O

Open System Interconnection (OSI), 11
Optimal bidding strategy, secure spectrum
  auctions. *See* Bidding strategy
Optimization problem:
  convex optimization problem as, 44, 47–50, 78, 80
  in latency-limited backhaul network, 113–114
  RA, with joint CA, 44–46, 50, 51–52, 80
  in rate-limited backhaul network, 112–113
  shadow price with, 57, 79–81
  sigmoidal-like function solving, 56
  UPF of, 52, 78–80
OSI. *See* Open System Interconnection

P

Paillier cryptosystem. *See also* MTSSA
  ciphertext created by, 19
  homomorphic properties of, 28, 32, 33, 41, 71, 85, 101
Paillier cryptosystem (Cont.):
  indistinguishability property of, 28–29, 39, 101, 106
  MTSSA leveraging, 28–29, 30–34, 39, 41
  as probabilistic public key encryption, 28
  properties of, 28–29
  secure spectrum auction, MTSSA, and, 3–4, 18, 28–34
  self-blinding property of, 29, 31, 39, 101, 102, 106
  in spectrum band allocation, 85–86
  THEMIS leveraging, 72
Pareto efficient, 24, 100
Payment method:
  of MTSSA, 19, 38
  in power scheduling auction, 100
  for spectrum sharing systems, IoT, 24–25
  in SPRING, 38

for VCG mechanism, 24, 85–86, 100
Performance analysis, 34, 40
of CSL, MTSSA, and MTSSA-FL, 35–38, 37f–38f
of MTSSA and SPRING, 38–39, 39*f*
Performance and security studies, IoT, 8–14
Physical-layer security methods, 7
Pilot channel, 23, 32, 85
Positive transfers, no, 24–26
Power consumption, 1
Power plant, 97, 99, 104–105, 105*f*
Power scheduling auction:
bid-rigging in, 101–102
payment method in, 100
for power plant, 97
power plant revenue and SM
satisfaction in, 104–106
secure gateway in, 98, 99f, 102–103, 106
in smart grid, 6
SMs in, 97–98, 98f, 101–104, 104*f*
President's Council of Advisors on
Science and Technology (PCAST), 4
Price per unit bandwidth:
of BSs, 79, 90
decreasing monotonically, 89–90, 90f, 95
negative proportionality, 81, 85
Pricing algor*i*thms, 12

Q

Quality of experience (QoE), 11
for active UE, 72–73
as allocation rate utility, 92, 92*f*
resource management solution for, 71
Quality of service (QoS):

in distributed RA algor*i*thm, 69 of LTE, 46
RA optimization in, 11, 46, 78

Y

RA. *See* Resource allocation
RA with joint CA, 131
in HetNet1, 60, 62f, 63–65, 64f, 67
in HetNet2, 66–67, 67f, 68*f*
optimization problem with joint CA, 44–46, 50–52, 80
Radio spectrum, 3, 8
allocation of, 1–2
demands and scarcity of, 4
reusability feature of, 9, 17, 75
secondary price auctions of, 10
UPF in, 11
Rate-limited backhaul network:
end-to-end latency and, 111–112
latency vs. processing time in, 115, 116f, 117
minimization problem in, 112–113
optimization problem in, 112–113
Real-time applications:
in HetNet1, 63–64
in HetNet2, 65, 69
logar*i*thmic utility function simulating, 59, 60*f*
true bidding with, 88–89, 92
Resource allocation (RA). *See also*
Distributed RA algor*i*thm; RA with joint CA
of CA, 2, 5–6, 14, 43, 71, 73
multicarrier, 11–12, 44, 50
multistage, 5, 64–65, 64*f*
nonzero, 5, 44, 46
QoS improving optimization, 11
UPF used by, 77–78

Revenue:
of auctioneer, 20, 24, 34–36, 37f, 38, 39f, 74, 88, 93, 94f, 105, 105*f*
Revenue (Cont.):
of power plant, 99, 104–105, 105*f*
traffic-dependent, 64, 65

S

SAPs. *See* Small cell access points
Secondary spectrum market, 8–9, 17
Secure gateway. *See also* Federal gateway
in bidding strategy, secure spectrum auctions, 76, 81
conflict table maintained by, 85–86
interference conflict graph by, 75–76, 75*f*
in power scheduling auction, 98, 99f, 102–103, 106
Secure spectrum auction design, MTSSA. *See also* Bidding strategy, secure spectrum auctions
frequency band allocation in, 29–30
Paillier cryptosystem in, 3–4, 18, 28–34
Sensing security transmission, 12–13
Sensor class, IoT, 109
Sensor report, for uplink networks secrecy, IoT, 2, 13, 107, 109–110, 112–114
Server, central:
decodability constraint at, 110–111, 112
in industrial IoT networks, 107, 109–110, 111–112, 113
Shadow price, 51
BSs calculating, 89–90, 90*f*
for eNodeB and UE, 53
in HetNet1, 64, 64*f*
minimization of, 52
with optimization problem, 57, 79–81

as rate of change, 83
Sigmoidal-like function, 56, 59, 60, 61*f*
Sigmoidal-like utility function:
curvature and inflection point of, 54–57
Hessian matrix of, 47, 49–50
natural logar*i*thm of, 50, 55–56
nonzero rate allocation in, 56
transmission cooperation at, 111
in true bidding values, 82–84, 88, 89f, 89*t*
in UPF, 44–45, 77–78
Small cell access points (SAPs):
central server, backhaul network, and, 109
LAP with, 107, 108f, 109, 111
processing and forwarding time in, 110–111
Small cells, 59
BSs, WSPs, and, 20, 21f–23f, 22, 34–35
in HetNet1, 60, 62f, 63–64, 63*f*
Smart grid, 6
design considerations for, 98, 99–101, 99*f*
homomorphic encryption in, 12, 15, 97, 99f, 101–103, 104f, 105–106, 105f, 106*f*
MATLAB code for IoT, 147–151
numerical results of, 104–106, 105f, 106*f*
power grid in, 98, 99*f*
power scheduling auction in, 97, 98, 99f, 101–104, 104*f*
scheduling mechanism, auction process, and, 2, 132
security and privacy considerations for, 100–101, 104
system model and design assumptions for, 98–99, 99*f*
Smart meters (SMs):
in power scheduling auction, 97–98, 98f, 101–104, 104*f*
security and privacy for, 100–101
traffic-dependent bidding value of, 64, 65, 99
SMs. *See* Smart meters
Social welfare, 25–26, 100

Spectrum auction, 2, 75f. *See also* Bidding strategy, secure spectrum auctions;
Spectrum sharing systems, IoT, leveraging secure spectrum auctions
BSs participation in, 72, 75–77
cellular networks, increasing demand and, 17–18
confidentiality, fairness, anonymity in, 3, 9
design, MTSSA, 27f, 28–34
economic properties of, 6–7
frequency assignment policy, 35
homomorphic encryption securing, 10
multiband, 20, 74
performance metrics of, 34–39, 37f–38f, 39*f*
secure, 3–4, 18, 28–34, 76, 131
Spectrum auction (Cont.):
spatial reuse property of, 18
truthfulness in, 26–27, 72
unsecured, 27*f*
Spectrum auction model:
frequency conflict graph of, 22–23, 22f, 75*f*
frequency reuse property in, 22
inference conflict graph of, 20, 21f, 22
for MTSSA, 23, 23*f*
for spectrum sharing systems, IoT, 20–23, 21f–23f, 21*t*
Spectrum band allocation. *See also* Radio spectrum
algor*i*thm (5), 86–87, 89, 91–92, 92*f*
economic properties of, 85–86
Paillier cryptosystem in, 85–86
procedure of, 86
secure gateway in, 85–86
Spectrum heterogeneity, 132
Spectrum pyramid, 19–20, 19*f*
Spectrum sharing, through secure and truthful auctions:

model of, 76–77, 76*f*
optimal mechanism, true bidding values in, 76–87, 76*f*
Spectrum sharing systems, IoT,
leveraging secure spectrum auctions, 4–6
design challenges in, 26–28, 27*f*
economic auction properties of, 25–26
key symbols for, 20, 21f, 22
MATLAB code for, 135–145
MTSSA in, 18–19, 28–34, 39–41, 40t, 41*f*
multitier, 3, 17, 41
numerical results and analysis of, 34–41, 37f–38f, 39f, 40t, 41*f*
optimal mechanism, true bidding values, and, 77–85
Paillier cryptosystem, 28, 30–34
payment method for, 24–25
spectrum auction model for, 20–23, 21f–23f, 21*t*
spectrum trading architecture for, 19–20, 19*f*
Spectrum utilization, 34–35
bidder satisfaction, auctioneer revenue, and, 34, 88, 93, 94*f*
MTSSA vs. MTSSA-FL in, 36, 37*f*
underutilized frequency bands vs., 36, 37f, 93, 94*f*
SPRING:
bid-rigging in, 39
bidding value submission of, 38
fraud in, 39
MTSSA compared to, 38–39, 39*f*
payment method in, 38
Stale data, 7
Stirling's formula, 40, 87
Subnet, 18
auction, 29–30, 41, 75–76
in frequency band allocation, 29–30
in frequency conflict graph of WSPs, 22f, 23, 75*f*

VCG auction in MTSSA, 32–34

T

TASC mechanism, 9
Temporary resources, BSs seeking, 71–72, 75, 77
THEMIS:
frequency bands and bidding values
issues with, 10
MTSSA compared, 40, 40t, 41*f*
Paillier cryptosystem leveraged by, 72
spectrum band allocation algor*i*thm
comparison with, 87
3GPP. *See* LTE third-generation
partnership project
Traffic-dependency, 13, 75, 122–123
bid pricing as, 64, 65
bidding value of SMs, 64, 65, 99
pricing by RA, 44
pricing in HetNet1, 65
revenue, 64, 65
Transmission cooperation, 111
True bidding price:
of BS k, 84
definition of, 73
with encrypted bidding value, 71
True bidding value, 131
BSs, demand, and, 71, 72
with delay-tolerant applications, 88–89
demand-based bidding price in, 81, 85, 91, 91f, 95
True bidding value (Cont.):
logar*i*thmic and sigmoidal-like utility
function in, 82–84, 88, 89f, 89*t*
in optimal bidding strategy, 77–85

with real-time applications, 88–89, 92
TRUST, 9
Truthfulness, 95
as incentive compatibility, 25
with MTSSA, 18
in spectrum auction, 26–27, 72, 76–87, 76*f*

U

UE. *See* User equipment
UMTS. *See* Universal Mobile Terrestrial System
Underutilized frequency bands:
of auctioneer, 21f, 22, 29, 34, 72, 93, 94*f*
BSs, WSP, and, 20, 21f–23f, 22, 34–35
federal government leasing, 18, 73
spectrum utilization vs., 36, 37f, 93, 94*f*
Universal Mobile Terrestrial System (UMTS), 11
UPF. *See* Utility proportional fairness
Uplink networks secrecy, IoT, 7, 15. See also M2M uplink communications
attack models in, 107, 108f, 114–115, 116f, 117
data transmission policy in, 109–111
encoding policy in, 109–110
forwarding policy in, 109, 110–111
IoT network model for, 108–111, 108*f*
latency-centric IoT uplink in, 111–114, 115, 116*f*
network connectivity in, 109
numerical results of, 115, 116f, 117
sensor reports with, 2, 13, 107, 109–110, 112–114
User equipment (UE), 4
active, applications in, 93
in distributed RA algorithm, 53

eNodeB serving, 45
fluctuation decay function in, 58
HetNets and applications for, 60, 62t, 65, 66f *i*th, 53, 58
MIMO capabilities of, 12
optimization problem of, 52
QoE for, 72–73
real-time or delay-tolerant application in, 59, 60f, 63–64, 65, 69
shadow price comparison by, 53
in spectrum trading scenario, 20
traffic of, 75
Utility proportional fairness (UPF), 43
in HetNet2, 67, 67f–68f, 69
logar*i*thmic utility function in, 44–45, 77–78
multicarrier cellular network problem of, 11–12, 44
objective function of, 46, 52
of optimization problem, 52
RA, CA, and, 5, 79–80
RA using, 77–78
radio spectrum, 11
sigmoidal-like utility function in, 44–45, 77–78

V

VCG auction. *See* Vickrey-Clarke-Groves auction
VERITAS, truthful mechanism
supporting dynamic spectrum market with, 9
Vickrey-Clarke-Groves (VCG) auction:
auctioneer revenue maximization with, 24
bid-rigging and greedy bidders in, 27, 27f, 100
favorable economic properties and vulnerabilities in, 6–7, 26–27
fraud in, 26–28, 27f, 100

incentive compatibility, individual rationality, and no positive transfers in, 24–26
in MTSSA subnet auction, 32–34
Vickrey-Clarke-Groves (VCG) auction
Pareto efficient in, 24, 100
payments with, 24, 85–86, 100
sealed secondary price auctions, bidding strategies, and, 9, 26
truthfulness concerns with, 26–27
Volumetric detection, 8, 13, 119, 121
DDoS with global, 124, 125f, 129*t*
DDoS with local, 124, 125f, 129*t*
device failure with global, 129*t*
device failure with local, 126, 128f, 129*t*
emergency scenario with global, 126, 129*t*
emergency scenario with local, 126, 127f, 129*t*
metrics, 122

W

WiMAX. *See* Worldwide Interoperability for Microwave Access
Wireless sensor networks, 1, 13–14
Wireless system providers (WSPs):
BSs, macro cells, small cells and, 20, 21f–23f, 22, 29, 34–35
coverage area of, 21f, 22
efficient spectrum sharing with, 17
frequency conflict graph of, 22f, 23, 75*f*
MTSSA with, 18
spectrum reuse among, 72
Worldwide Interoperability for Microwave Access (WiMAX), 11
WSPs. *See* Wireless system providers

Z

Zero rate, 11
in distributed RA algor*i*thm, 53
in HetNet1, 62f, 63
in HetNet2, 67, 67f–68f